Master i Rettsvitenskap

Forholdet mellom datalagringsdirektivet og den europeiske menneskerettskonvensjon artikkel 8

Innhold

1 Innledning

1.1 Problemstilling og tema

Den rettslige problemstillingen jeg drøfter i min oppgave, er hvorvidt man kan innføre EU-direktiv 2006/24/EF[1] (heretter datalaringsdirektivet) uten at det vil foreligge motstrid med den europeiske menneskerettskonvensjon[2] (heretter EMK). Mer spesifikt vil jeg søke å harmonisere de krav EMK art. 8 stiller til rett til respekt for privatliv og korrespondanse med de krav datalagringsdirektivet stiller til lagring av trafikkdata for å forebygge og etterforske grov kriminalitet. I denne prosessen vil forholdet mellom de proporsjonalitet- og nødvendighetskrav som kan utledes av EMK art. 8 og den nytteeffekten direktivet utgjør være et sentralt vurderingstema.

Datalagringsdirektivet ble vedtatt 15. mars 2006. Direktivet innebærer at medlemsstatene via nasjonal lovgivning skal sikre at trafikkdata fra Internettrafikk, mobiltelefoni og fasttelefoni skal lagres fra 6-24 måneder. Trafikkdata er bl.a.lokasjonsdata, oversikt over hvem man kommuniserer med, når man kommuniserer o.l. Disse dataene skal være tilgjengelig for bruk i etterforskning og forebygging av grov kriminalitet. Direktivet hadde i utgangspunktet to uttalte hovedformål. Det første var etterforskning og forebygging av grov kriminalitet. Det andre var å gjøre konkurransesituasjonen blant kommunikasjonsleverandører i EU mer rettferdig. Direktivet medfører at borgernes kommunikasjonsvaner og bevegelsesmønster blir lagret i databaser som kan systematiseres og forskes på. Politi- og påtalemyndigheter vil sådan kunne utlede innholdslignende konklusjoner om borgerne av dette materialet.

EMK art. 8 på sin side, gir borgerne en rett til respekt for privatliv og korrespondanse. Denne artikkelen beskytter også andre sider av privatliv, familieliv o.l, men dette vil i mindre grad være relevant for min oppgave. En innføring av direktivet, vil utgjøre et inngrep i disse rettighetene. Jeg vil i min oppgave vurdere om dette inngrepet kan gjøres i tråd med de unntaksregler som foreligger i andre ledd av art. 8. Hensynet til personvern og privatliv må balanseres opp mot behovet for å bekjempe grov kriminalitet. Denne vurderingen vil som tidligere nevnt komme på spissen når det gjelder vurderinger rundt proporsjonalitet og nødvendighet.

En prosess der man søker å harmonisere to folkerettslige forpliktelser, innebærer fortolkning av de aktuelle rettsregler og eventuell praksis som tilhører disse. Når det gjelder EMK vil jeg søke å gjøre dette ved å trekke inn relevant rettspraksis fra den europeiske menneskerettsdomstol (heretter EMD) for å med større presisjon avgjøre hva art. 8 innebærer. Tilsvarende vil jeg for å klargjøre hvilke plikter direktivet medfører, se på forskjellige løsninger fra andre EU-land i lys av direktivets ordlyd.

1 DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

2 Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14 Rome, 4.XI.1950

Det sistnevnte belyser dog en svakhet med min problemstilling. Jeg skal ikke holde en aktuell og konkret gjennomføringsmodell opp mot de krav EMK art. 8 stiller, men derimot en potensiell og dermed abstrakt norsk gjennomføring. Dette vanskeliggjør klare konklusjoner og presise avveininger. Jeg har søkt å avhjelpe dette ved å se på praksis fra andre EU-land, tolke ordlyden i direktivet og se på potensielle gjennomføringer som møter de minimums- og maksimumskrav direktivet stiller.

Det er ikke rom i oppgaven til å gå nærmere inn på problemstillinger rundt en eventuell bruk av reservasjonsretten i forhold til direktivet. Dette ville uansett ikke berørt min problemstilling nevneverdig.

Den avgjørende problemstillingen etter dette, blir å avgjøre om direktivet er et nødvendig og proporsjonalt inngrep med det formål å forebygge og etterforske grov kriminalitet

1.2 Bakgrunn for valg av tema

Få har vel gått glipp av debatten rundt den eventuelle innføringen av datalagringsdirektivet i Norge. Debatten har favnet svært bredt og engasjert politikere, jurister, samfunnsvitere og spesielt i sosiale medier har diskusjonen vært fremtredende. Sentralt i den nasjonale debatten har Arbeiderpartiet, KRIPOS, Datatilsynet og bl.a.NRKs jurister stått. I Europa forøvrig har det også vært stor strid rundt innføringen av direktivet og Irland har sågar gått til sak for EU-domstolen for å få avskrevet direktivet som følge av at det ikke er lagt under riktig EU-pillar. Dette ble avvist av EU-domstolen. Tilbake til den nasjonale debatten, har mange av ståstedene vært polarisert. Man har Helga Pedersen på en side, med sitt "Redder vi ett barn, er det verdt det"-utsagn[3]. Der det hevdes at direktivet er verdt det om det fører til at et barn reddes fra misbruk. På motsatt side i debatten har man hatt tidligere leder for Datatilsynet, Georg Apenes, som ser på direktivet som "totalitært svermeri"[4]. Motpoler av denne art har preget debatten både på seminar, i avisene og media forøvrig.

I tillegg har diskusjonen rundt direktivet igangsatt debatten om Norges bruk av reservasjonsretten i forhold til EU. Mange aktører mener at Norge må bruke denne vetoretten, andre mener at det vil være et europapolitisk selvmord for Norge å bruke denne her.

Debatten rundt direktivet har også en plass i en bredere internasjonal debatt om kampen mot terrorisme og forholdet til personvern. Det er liten tvil om at terroraksjonen mot World Trade Center i 2001 og påfølgende aksjoner i bl.a. Madrid og London gav pådriverne for direktivet mye ammunisjon og satte hjulene i gang for alvor[5]. Dette kulminerte i at direktivet ble vedtatt nesten nøyaktig to år senere. Parallelt kunne man se en lignende utvikling i USA[6] der myndighetene i løpet av 2005-2006 presset på for å få tilgang på lagrede trafikkdata som et verktøy i kampen mot terrorisme.

3 Høyre for light-versjon av datalagringsdirektivet, Aftenbladet
4 Totalitært svermeri (22.12.2006) Georg Apenes
5 Se bl.a. Declaration on Combating Terrorism of 25 March 2004 som kom rett i etterkant av bombingen i Madrid
6 Se bl.a. "Gonzales pressures ISPs on data retention" - Declan McCullagh, CNET

Et av hovedinntrykkene jeg som jusstudent satt igjen med etter debatten, var at svært få diskuterte emnet på et juridisk nivå. Det var i stor grad en veldig politisert debatt der vurderingstema var vage, sjelden godt definerte. De eventuelle juridiske problemstillingene direktivet reiste ble sjelden diskutert i dybden. Det var i lys av dette jeg bestemte meg for å skrive en oppgave om direktivet og dets forhold til den europeiske menneskerettskonvensjon. For meg fremstod det som viktig å klargjøre forholdet mellom disse to folkerettslige forpliktelsene.

1.3 Oppgavens oppbygning

Etter denne første delen av oppgaven, der jeg presenterer problemstillingen, årsak for valg av problemstilling og en rask oppsummering av oppgavens oppbygning. Viderevil jeg fortsette med å presentere datalagringsdirektivet. Jeg vil i denne delen av oppgaven se på direktivteksten og klargjøre hvordan jeg tolker denne. I den tredje delen av oppgaven, vil jeg se på ulike gjennomføringsmodeller i et utvalg av medlemsstater. Dette for å klargjøre hvordan direktivet blir gjennomført i praksis. Dette er empirien som tildels utgjør grunnlaget for drøftelser rundt aktuelle gjennomføringsmodeller i Norge. Jeg vil også se på to nasjonale dommer som omhandler direktivets gjennomføring i de respektive statene i denne delen. I tillegg går jeg gjennom empiriske data rundt bruken av trafikkdata i forskjellige land. Disse data får betydning i den senere proporsjonalitetsdrøftelsen. I den fjerde og femte delen ligger hovedtyngden av drøftelsene. Her presenterer jeg EMK art. 8 og dens forhold til direktivet. Hovedvekten vil ligge på lovkvalitetsspørsmålet og proporsjonalitets- og nødvendighetsdrøftelser. Relevante problemstillinger vil drøftes fortløpende i disse to delene.

1.4 Metode

I forbindelse med tolkning av direktivet, EMK og praksis fra EMD har jeg basert meg på den tradisjonelle juridiske metode slik den bl.a. fremgår av Harris[7] og Kjølbro[8]. Jeg har forsøkt å tolke konvensjonsteksten i tråd med den praksis som foreligger fra EMK og har tilsvarende søkt å bruke de enkelte nasjonale gjennomføringsmodeller som veiledning når det har oppstått usikkerhet i tolkningen av direktivet.

Det som er verdt å si noe om, er en del av de andre kildene jeg bruker og hvordan jeg bruker dem. Når det gjelder dommene fra tyske og rumenske forfatningsdomstoler, har jeg kun tilgang på uoffisielle oversettelser, noe som kan være en feilkilde. I tillegg har jeg begrenset kjennskap til både rumensk og tysk rettskildelære i forhold til den praksis de har ved sine forfatningsdomstoler, noe som også kan være en potensiell feilkilde. Dette har jeg forsøkt å ta høyde for i mine drøftelser. Videre er det i hovedsak uoffisielle oversettelser av de nasjonale implementeringslover jeg har hatt til rådighet, noe som også kan være en kilde til misforståelser og/eller feiltolkning av flertydigheter.

7 Law of the European Convention on Human Rights, 2009
8 Kjølbro, 2010

Når det gjelder statistikk vil jeg referere direkte til kildene når jeg bruker statistikk, men jeg kan likevel kort nevne at hoveddelen av statistikken jeg bruker kommer fra Danmark, Norge, Sverige og Tyskland. Det er vanskelig å sammenligne disse kildene da noe er intervjuer av representanter for den utøvende myndighet i politi og påtalemyndighet, noe er data rundt uthentingsfrekvens (og hvilke saker data blir søkt uthentet) og andre kilder er politi- og påtalemyndighetenes egne uttalelser om effektivitet og nyttighet. Alt dette kan være mulige feilkilder og/eller bidra til å svekke dataenes vekt, noe jeg også har forsøkt å ta høyde for i de tilhørende vurderinger.

1.5 Begrepsliste

Før jeg går nærmere inn i materien, vil jeg første presentere noen begreper som vil kunne gjøre det enklere å forstå deler av direktivet. Ordlisten er ikke uttømmende, men vil bidra til større forståelse for de som ikke nødvendigvis har tung teknisk forståelse.

ISP: Internet Service Provider, Internettleverandør. En Internettleverandør er selskapet som står for den rent fysiske oppkoblingen fra brukerne og opp til Internett Disse leverer også epost og bredbåndstelefonitjenester, disse skiller seg fra Internettbaserte epost- og telefonitjenester som f.eks.. Gmail, hotmail o.l.

IP-adresse: En IP-adresse er en adresse som kan sammenlignes med et telefonnummer. Hver datamaskin i et nettverk blir tildelt en IP-adresse som representerer denne i nettverket og brukes for å rute kommunikasjon til riktig enhet. IP-adresser skiller seg dog fra telefonnummer på flere områder. En IP-adresse kan f.eks.. representere en hel rekke forskjellige nettsider. Dette fungerer slik at en server (med en IP-adresse) samtidig tjener flere forskjellige sider. Dette innebærer at man ikke nødvendigvis kan spore opp hvilke nettsider en bruker surfer på, selv om man får tak i en pi-adresse. Andre momenter som kan være verdt å nevne er at man kan ha interne IP-adresser på et eget nettverk, som ikke kommuniseres ut til verden. Her vil det kun være en IP-adresse som ses utenfra når maskinene på det interne nettet kommuniserer med eksterne maskiner. Om man har et stort internt nett (slik f.eks.. UiO har med sitt studentbynettverk) er det ikke nødvendigvis slik at administrator av dette nettverket kan spore hvem som står bak en gitt kommunikasjon til en gitt tid om slikt ikke lagres av de som er ansvarlige for det interne nettverket. Mange nettverk bruker det som kalles dynamiske IP-adresser der maskinene på det interne nettverket tildeles IP-adresser fra en gruppe intern-adresser, og hvor man med jevne mellomrom (og ofte når man logger på nettverket) får en ny adresse.

Portnummer: Et portnummer identifiserer hva slags kommunikasjonsport en kommunikasjon har gått over. Dette er ikke nødvendigvis en sikker metode, men mange av de kommunikasjonsformene vi bruker har faste porter, og man kan dermed fra portnummer-informasjon vurdere om det er mest sannsynlig at det har vært epost-kontakt, ordinær nettlesing eller andre lignende typer trafikk.

Protokoll: Begrepet protokoll i en teknologisk kontekst, kan sammenlignes med diplomatisk protokoll. Man har forskjellige systemer som innad snakker forskjellige språk, men som må ha felles protokoller for å kunne kommunisere på tvers av disse systemgrensene. Dette gjør at vidt forskjellig programvare kan kommunisere uhindret. En eposttjener fra Microsoft følger epost-protokollen, og kan dermed kommunisere med en tilsvarende tjener fra f.eks. Mozilla.

Internettbasert epost: Direktivet skiller mellom epost-tjenester hos den lokale Internettleverandøren og eposttjenester man får på Internett, eksempler på sistnevnte er f.eks. Gmail og hotmail. Slike online eposttjenester omfattes ikke per dags dato av direktivet. Derimot er altså epost-tjenester levert av lokale nettleverandører der man kan assosiere epostadresser og kontoer med registrerte navn og adresser omfattet.

Internettelefoni: En løsning tilsvarende den for Internettepost gjelder også for Internettelefoni. De tjenestene man har fra lokale tilbydere, Telenor bredbåndstelefoni f.eks., blir omfattet av direktivet. Tjenester som Skype derimot, som er nettbaserte og ikke lokale, vil ikke omfattes av lagringsplikten.

IMSI-nummer: International Mobile Subscriber Identity er et unikt nummer som tilhører simkortet alle har i sine GSM/UMTS-telefoner (mobiltelefoner). Dette nummeret gjør at man på verdensbasis kan spore simkort uavhengig av hvilken telefon de tilhører. Simkortet gjør at mobiltelefoner kan kommunisere med det nettverket simkortet er programmert for.

IMEI-nummer: International Mobile Equipment Identity tilsvarer IMSI, med den forskjell at det her er selve mobiltelefonen som registreres med et unikt nummer. Hver eneste enhet har sitt eget unike registreringsnummer og kan sådan spores uavhengig av simkort/IMSI-nummer.

SMS-tjenester: SMS er den tjenesten de fleste av oss bruker når vi skal sende ordinære tekstmeldinger til andre mobiler.

EMS-tjenester: Noen år tilbake utviklet noen av mobiloperatørene en tjeneste med lav oppløselige animasjoner/bilder som kunne sendes som meldinger til andre som hadde mobiler som støttet denne teknologien. I Skandinavia slo aldri denne teknologien særlig an, men i andre deler av Europa blir den mer brukt.

MMS-tjenester: Multimediameldinger hvor man kan legge ved tekst, bilder, lyd, filmer o.l. Dette kan man sende til en eller flere mottagere.

2 Presentasjon av datalagringsdirektivet

2.1 Innledning

Etter flere års dragkamp ble det såkalte datalagringsdirektivet vedtatt 15. mars 2006.[9] Da hadde EU gått hele veien fra personvernorienterte og databeskyttende direktiver på 90-tallet, til det mer overvåkningsrettede og lagringsvennlige som fikk uttrykk i dette direktivet.[10] Det har vært en relativt lang politisk prosess og initiativene fra tilhengerne av direktivet har vært mange, det var dog ikke, som nevnt over før flere terroraksjoner at initiativene fikk momentum.[11] Den offisielle hensikten med datalagringsdirektivet var todelt. For det første så EU at flere av medlemsstatene i stor grad benyttet seg av unntaksreglene i databeskyttelsesdirektivet.[12] Datalagringsdirektivet skulle opprinnelig harmonisere forholdene for tele- og datakommunikasjonstilbydere. Det hadde oppstått en situasjon der forskjell i datalagringsregler utgjorde en konkurransevridning. Tilbydere i land der det ikke var utstrakt bruk av datalagring hadde merkbare økonomiske fordeler i forhold til tilbydere i medlemsland med mer utstrakt bruk av datalagring. Denne årsaken til harmoniseringen av regelverket fremstår mer eller mindre som konstruert i den grad det ikke er fastslått i direktivet om tilbyderne selv eller statene skal stå for merutgiftene, og at det allerede har blitt sprikende praksis i de forskjellige medlemslandene.[13]

For det andre ville EU også søke å gi medlemsstatene mer samsvarende verktøy på tvers av landegrensene i kampen mot grov kriminalitet. På begynnelsen av 2000-tallet var det i hovedsak stor motstand mot denne typen inngrep, grunnet personvernhensyn. Noe både Data Protection Working Party og European Data Protection Supervisor satte søkelyset på i den videre prosessen.[14] Mange andre organisasjoner og medlemsland stilte seg også kritisk til gjennomføring av utstrakt lagring. Etter 11. september 2001 ble påtrykket fra USA større, det etter hvert så berømte brevet fra Bush til Guy Verhofstadt, daværende EU-president, er i så måte betegnende på situasjonen.[15] Støtten til datalagringsdirektivet fra politisk hold innad i EU ble enda sterkere både som følge av bombingen i Madrid i 2004 og bombingen av metroen i London i 2005. England satt med presidentskapet høsten 2005. De jobbet også aktivt med å skape støtte og legge veien klar for direktivet i denne perioden. Direktivet ble det

9 DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

10 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

11 Se bl.a. Declaration on Combating Terrorism of 25 March 2004 som kom rett i etterkant av bombingen i Madrid.

12 2002/58/EC DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 (Et direktiv som omhandler datatilsyn og databeskyttelse for EU-borgerne. Dette direktivet er en sentral del av personvernlovgivningen i EU)

13 Evaluation of directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communication s. 6

14 Bignami, 2007, s240.

15 http://www.zdnet.co.uk/news/networking/2001/11/05/bush-lobbies-eu-to-drop-traffic-data-retention-ban-2098596/

raskest gjennomførte i historien, kun tre måneder tok det fra det ble skissert til et vedtak forelå.[16] Det er vanskelig å komme med en uttømmende analyse av hvorfor holdningene blant flere medlemsland endret seg så radikalt i denne tidsperioden, men de tre store terrorhandlingen (New York, Madrid og London) var nok sterkt medvirkende. Utover høsten 2005 ble det etter hvert klart at datalagringsdirektivet mest sannsynlig ville gå gjennom og i mars 2006 ble det vedtatt. Hva er så datalagringsdirektivet, hvilke konsekvenser vil det få? Hva innebærer det egentlig? Jeg vil i det følgende gå gjennom hvilke data som skal lagres, hva disse data kan brukes til, hvem som kan hente ut data, hvilke kontrollmekanismer som skal etableres, hvor lenge data skal lagres osv. Jeg vil også kort informere om de forskjellige gjennomføringsmodellene som har blitt brukt i forskjellige medlemsland på forskjellige områder av direktivet. Kjernen i direktivet er at statene må iverksette tvungen lagring av det som kalles trafikkdata. Disse data skal på sin side lette etterforskning av grovere kriminalitet og hjelpe myndighetene til å motvirke terrorisme.

Jeg vil gå forholdsvis grundig gjennom direktivteksten og klargjøre min fortolkning av denne. Dette for å gi leseren bakgrunn for å forstå både nasjonale implementeringslover bedre, men også for å tilrettelegge for drøftelser rundt mulige tolkninger av direktivet som kan harmoniseres med EMK art. 8.

2.2 Hvilke brukeres data skal lagres

Dette fremgår av direktivets art. 1 andre ledd. Alle data fra både fysiske og juridiske personer skal lagres, det er sådan ingen unntak for bedrifter eller andre juridiske personer. Likevel er det som jeg vil komme inn på senere et unntak for bedriftsinterne nett og for situasjoner der det ikke er snakk om kommersielle aktørers nett.

2.3 Oversikt over hvilke data som skal lagres

Kort fortalt skal informasjon om hvem som deltar i en kommunikasjonsøkt, hvor de befinner seg og hvilken form for kommunikasjon som brukes lagres. Jeg skal gå nærmere gjennom detaljene rundt dette under. Jeg vil først prøve å komme med noen eksempler på hva dette kan innebære. Jeg er en student på 27 år, jeg har en smarttelefon og bruker Internett både på stasjonære, bærbare og håndholdte enheter jevnlig. Jeg bruker tjenester som Twitter, Facebook, Gmail, Flickr o.l. både hjemme og på telefonen. Jeg har forsøkt å registrere egen bruk over noen døgn for å kunne skissere hvor ofte og hva som lagres om meg. For det første bruker jeg ordinær telefonkommunikasjon sjelden, så de samtalene som lagres er i hovedsak til familie, kjæreste og jobb. Mer sentralt er at telefonen min automatisk oppdaterer ting som Facebook, eposten min o.l. hele dagen. Det innebærer at ca. hvert 10-15. minutt så kommuniserer telefonen min med Internett og dermed vil hvor jeg befinner meg kartlegges

16 Digital Rights Ireland, 2005, http://www.digitalrights.ie/2005/12/

med en forholdsvis ekstrem presisjon. Dette gjør at mine reisevaner, hvor jeg befinner meg til enhver tid og annen info er tilgjengelig. Juristen Christian Elind har fått utlevert sine geografiske trafikkdata fra leverandør.[17] Her ser man at et moderne kommunikasjonsmønster medfører en ekstremt detaljert geografisk oversikt. Dette er en tendens som nok vil utvikle seg til å bli mer og mer omfattende, noe som i seg selv er en faktor man må ta med i vurderingen av direktivet.

Det er såkalte trafikkdata som skal lagres, det inkluderer informasjon om identifiserbare kommunikasjonsdeltagere på telekomtilbyderes nett. Det fremgår av art. 5 hva som faktisk skal lagres.I direktivet har man delt inn i data nødvendig for å identifisere utgangspunktet for en kommunikasjonsøkt, mottager for en kommunikasjonsøkt, nødvendige data for å identifisere tid, dato og varighet, nødvendige data for å identifisere typen kommunikasjon, data for å identifisere brukers kommunikasjonsutstyr (Eller det utstyr brukerne simulerer at de bruker. Det er flere måter en bruker kan maskere sitt reelle utstyr og simulere bruk av annet utstyr.), og lokasjonsdata for mobiltelefoner.

Hva ligger så i alle disse kategoriene? Jeg vil gå gjennom hvert enkelt underpunkt fra direktivet og klargjøre hvordan jeg tolker det og hvilke data som i dagens kommunikasjonsnett vil bli lagret. Et poeng som kan være verdt å nevne, er den teknologiske utviklingen når det gjelder kommunikasjon. Måten vi kommuniserer på, både når det gjelder programvare (Facebook,, Gmail o.l.) og maskinvare (Internett, mobilnett) vil endre seg de neste tiår. Dette er en utfordring for de fleste innføringsmodeller.

Når det gjelder telefonkommunikasjon, både fastlinje og mobil, vil følgende data være nødvendige: oppringende telefonnummer, navn og adresse registrert på dette nummer. Nummer (hvis flere: alle) som blir oppringt, viderekoblingsinfo om alle nummer samtalen eventuelt blir rutet til, navn og adresse registrert på alle involverte nummer. Samtalens varighet vil også bli lagret (start og sluttid). Type telekommunikasjon innebærer informasjon om hvorvidt det er SMS, EMS, en ordinær telefonsamtale eller lignende som kommuniseres. For mobiltelefoni skal i tillegg IMSI- og IMEI-nummer til begge samtaleparter (eller flere) lagres. For kontantkort skal i tillegg lokasjonsdata for opprinnelig aktivering samt tidspunkt for denne lagres for å ha oversikt over hvor og når et slikt kort ble aktivert. For mobiltelefonsamtaler skal celleinfo med lokasjonsdata lagres både ved starten av samtalen, i løpet av og på avslutningen av samtalen lagres for begge parter. En typisk samtale mellom en Netcom-bruker og en Telenor-bruker der brukeren som ringer fra fasttelefon og mottageren har mobiltelefon vil føre til at følgende data lagres: Hos fasttelefonbrukeren vil navn og adresse, telefonnummer ringt fra og til, varighet på samtale og type abonnementsservice lagres, hos mobiltelefonbrukeren vil navn og adresse, nummer oppringt fra og til, IMSI og IMEI-nummer og lokasjonsdata for hele samtaleperioden lagres. Man vil dermed spesielt for mobiltelefoni få en situasjon der alle bevegelser gjort kan kartlegges såfremt man bruker telefonen, men også for bærbare datamaskiner kan IP-adressen brukes for å kartlegge bevegelser. Bruker man en kombinasjon av IP-adresser fra en bærbar datamaskin samt lokasjonsdata fra en mobiltelefon, kan man med forholdsvis god presisjon kunne kartlegge en persons bevegelsesmønster.

17 Elind, 2010, http://trollkar.blogspot.com/2010/12/datalagringsdirektivets-loggfring-i.html

Et annet moment er såkalte bedriftsinterne nett. Det fremgår av art. 3 at det kun er offentlig tilgjengelige og kommersielle nett som har lagringsplikt. Konsekvensen av dette er at nett som UiO-nettet og andre større, lukkede nett, ikke omfattes av lagringsplikten. Som et godt eksempel kan man da peke på de forskjellige studentbyer som har Internett gjennom UiO. Disse vil ikke omfattes av lagringsplikten da de faller inn under UiO-nettet og dette, slik jeg har tolket direktivet, vil defineres som et bedriftsinternt nett. I tillegg vil en hel rekke større bedrifts- og organisasjonsnett falle utenfor. I tillegg til de store universitetsnettene har man store bedrifter og store organisasjoner som sykehus o.l som vil falle utenfor lagringsplikten.

Når det gjelder Internettbruk vil jeg dele inn i tre forskjellige kategorier: Internettelefoni, epost og ordinær bruk av Internett.

Når det gjelder Internettelefoni skal følgende data lagres om avsender av kommunikasjon: tildelt brukerID, brukerID som tilhører enhet ved oppkobling mot det ordinære telefonnettet, navn og adresse til abonnent eller bruker av en tildelt IP-adresse, brukernavn eller telefonnummer ved tilkoblingstidspunkt. På mottagersiden skal brukernavn, telefonnummer, navn og adresse på abonnent eller bruker av telefontjenesten lagres. I tillegg skal tjenestetype lagres, her skal informasjon om tjenestetype lagres, slik jeg tolker praksis fra medlemsstatene innebærer dette transportprotokollinformasjon. Tid og sted for av- og pålogging skal også lagres, samt oppkoblingsinformasjon relatert til analoglinje (telefonnummer) eller DSL-linje (oppkoblingspunkt).

For Internettepost vil reglene ligne mye på de som gjelder for Internettelefoni. Følgende data skal lagres om avsender av kommunikasjon: tildelt brukerID og navn og adresse til abonnent eller bruker av en tildelt IP-adresse. På mottagersiden skal brukernavn, navn og adresse på abonnent eller bruker av eposttjenesten lagres. Forøvrig skal også tidsinformasjon for på- og avloggingsinformasjon lagres, IP-adresse, uavhengig om den er statisk eller dynamisk. Også ved bruk av Internetteposttjenester skal tjenestenavn lagres, slik jeg tolker direktivet vil det også her være tilbyder og abonnementsinfo som skal lagres, f.eks. ”Telenor privat epost” eller ”Canal Digital bredbånd, tilhørende epost”. Alternativt kan det være at man i direktivteksten sikter mot protokoll- og portinformasjon. Det vil medføre en mer detaljert lagring og man vil da få kjennskap til hva slags kommunikasjon som føres, er det SSH, FTP, epost eller annen kommunikasjon som skjer? Gjennomføringsmodellen i Danmark indikerer at det sistnevnte alternativet er en logisk tolkning, da de krever logging av nettopp protokoll- og portinformasjon hos avsender og mottager. Avslutningsvis skal det også her logges oppkoblingsinformasjon. For analoge linjer skal telefonnummer lagres, for DSL-linjer skal oppkoblingspunkt lagres.

Når det gjelder ordinær bruk av Internett er det mindre utstrakt lagring. For avsender skal de samme data som ved internsettepost og Internettelefoni lagres: tildelt brukerID, navn og adresse til abonnent eller bruker av en tildelt IP-adresse. Slik jeg tolker direktivet skal ikke data lagres om mottager. I kapittelet om avsender er overskriften følgende: ”concerning Internet access, Internet e-mail and Internet telephony:”, når det gjelder mottager av

datatrafikk er derimot overskriften denne: ”concerning Internet e-mail and Internet telephony:”. Slik jeg tolker direktivteksten, og da spesifikt utelatelsen av ”Internet access” i den sistnevnte overskriften, er det ikke krav om lagring av IP-adresser eller annen info for mottager hos avsenders ISP. Det som derimot skal lagres er tidspunkt for på- og avlogging med kompensering for tidssone og informasjon om den analoge eller digitale oppkoblingen (telefonnummer og oppkoblingspunkt. Som en kommentar har innføringen av direktivet i bl.a.Danmark lagt til grunn en annen tolkning av dette punktet. I Danmark lagrer man IP-adresse til både avsender og mottager av Internettkommunikasjon, samt port- og protokollinfo. Dette er en utvidelse i forhold til min tolkning av direktivteksten og griper ytterligere inn i borgernes rettigheter etter EMK art. 8.

Det kan nevnes at også samtaler der man ikke får svar vil medføre lagring, dette fremgår av direktivets art. 3 andre ledd. Samtaler der avsender ikke får koblet til nettet vil derimot ikke kreve logging. Igjen kan jeg raskt kommentere at måten direktivet har blitt gjennomført i Danmark, skiller seg fra min tolkning av direktivet, her blir også samtaler som ikke kobles, lagres såfremt ikke-oppkoblingen er en følge av teknisk svikt.

Det er altså en hel rekke data som lagres, både om type tjenester vi bruker, hvem vi kommuniserer med, når vi bruker dem, hvor vi bruker dem og hvor lenge vi bruker dem. Hva er det så som faller utenfor direktivets rekkevidde? Det er flere tjenester som vil falle utenfor direktivets rekkevidde, i en særstilling står såkalte webløsninger. Tjenester som Skype, Gmail, Hotmail, Facebook og lignende, vil ikke få lagringsplikt slik jeg tolker direktivet. Ordlyden i art. 3 tilsier at det kun er lokale leverandører av tjenester som skal lagre data. De aller fleste internasjonale tilbydere av epost og Internettelefoni har tjenere utenfor EUs grenser, noe som vil medføre store praktiske problemer med jurisdiksjon i forhold til slik lagring. Det innebærer at Telenors epost-tjeneste til sine kunder vil måtte medføre lagring, samtidig som de samme brukernes parallelle bruk av Gmail ikke vil medføre lagring utover lagring av IP-adresse lokalt. Det samme gjelder for bredbåndstelefoni, der brukere av Telenors bredbåndstelefoni vil få lagret abonnementsinfo, telefonnummer, varighet av samtaler etc (som nevnt over), vil den samme brukerens bruk av Skype ikke generere data utover abonnementsinfo, IP-adresser o.l. for brukeren selv. Det eneste man kan hente ut av informasjon etter bruk av Gmail er dermed at brukeren har logget på Internett på et gitt tidspunkt fra en gitt node. Store deler av befolkningens bruk av sosiale tjenester, eposttjenester og Internettelefoni vil dermed ikke lagres som følge av dette.

Hva ligger så av informasjon i disse trafikkdata? De data som lagres vil skape et relativt detaljert bilde av hvor vi ferdes, hvor ofte vi kommuniseres, hvem vi kommuniserer med og hvordan. En gjengs borger i Norge bruker mobiltelefon og Internett relativt aktivt. Dette vil føre til at man i stor grad kan kartlegge hvor borgerne beveger seg til enhver tid. En ting er at det ved mobilbruk eksplisitt skal lagres bevegelsesdata, en annen ting er at IP-adresser, uavhengig om de er dynamiske eller statiske, vil kunne avsløre hvor også stasjonær/ordinær Internettrafikk kommer fra rent geografisk. Dette brukes bl.a. av Google når de tilpasser annonsering til geografisk plassering. En slik peiling vil ikke være fullt så presis som de data man får fra mobilbruk, men man får et relativt nøyaktig geografisk treff også med denne teknologien. Spesielt når teknologien stadig utvikles og vi får flere og flere håndholdte enheter, så vil en slik lagring føre til en stadig mer detaljert kartlegging av bevegelsesmønster.

Som en avslutning kan jeg raskt sammenfatte grovt hvilke data som skal lagres:

- Adresse, navn og kontaktinformasjon forøvrig på abonnenter som bruker tjenester.
- Tjenestetype/IP-adresser for Internettelefoni og eposttjenester.
- Lokasjon- og tid/dato-info om all aktivitet. (Pålogging, avlogging, samtalevarighet etc).
- IMEI/IMSI-nummer for mobiltelefonbrukere

2.4 Oversikt over hva lagrede data kan brukes til

Det fremgår av formålet i art. 1 at lagrede data skal brukes for å oppdage, etterforske og reise tiltale for "serious crime". Definisjonen av "serious crime" er overlatt til de forskjellige medlemslandene. Videre fremgår det av art. 4 at medlemslandene selv har ansvaret for at regelverk opprettes og at det kun blir mulig å få tilgang på data i konkrete tilfeller og i henhold til de retningslinjer og føringer EMK art. 8 innebærer. Dette legger hovedvekten av ansvaret for å definere regler for uttak av data på statene selv. De politiske signaler som de forskjellige medlemslandene har sendt varierer sterkt. Hovedlinjen synes å være at grov kriminalitet og terrorisme er det lagrede data skal brukes til. Slik jeg tolker direktivteksten, er kravet til bruksområde et minimumskrav. Det innebærer at det ikke bryter med direktivet om statene velger å utvide bruksområdet for de lagrede data. Dette innebærer f.eks. bruk i sivile saker, noe man allerede har sett eksempler på.

Jeg vil nå se nærmere på hvordan bruk av trafikkdata reguleres i noen europeiske land. Den danske løsningen ved implementering av datalagringsdirektivet, er sammensatt. Det er flere krav som må møtes før politiet kan hente ut data jf den danske retsplejeloven §§781-782.[18] For det første må det være bestemte grunner til å anta at det kommuniseres til eller fra en mistenkt, for det andre må bevisene antas å ha avgjørende betydning for etterforskningen, etterforskningen må gjelde en lovovertredelse med en strafferamme på 6 år eller mer, eventuelt gjelde en liste over spesifikke lovbrudd. Videre må man uansett foreta en forholdsmessighetsvurdering slik at de tiltak man gjør og de ulemper og krenkelser det innebærer ikke utveier fordelene ved inngrepet. I Finland har de en lignende ordning, men der er kravet til strafferamme på 4 år. Det kan synes å være en gjeldende norm blant medlemsstatene at en strafferamme på 3-6 år samt noen spesifikke lovbrudd som blir nærmere spesifisert i nasjonal lovgivning er den valgte løsning. Dette er også den norske foreslåtte løsningen i høringsnotatet fra departementet, der legges grensen på 3 år, i tillegg nevnes en rekke spesifikke lovbrudd som også vil omfattes av muligheten til å hente ut lagrede trafikkdata. Dette gjelder spionasje, terrorvirksomhet, datakriminalitet og en del former for

18 LBK nr 1053 af 29/10/2009 - Bekendtgørelse af lov om rettens pleje [Danmark]

organisert vinningskriminalitet og barneporno samt lignende lovbrudd. Det er altså ganske varierende hva de forskjellige land legger i ”grov kriminalitet” og ikke minst i hvor bredt skjønnsrom som gis de nasjonale domstoler eller politi- og påtalemyndigheter. Som en hovedregel synes det dog å være varierende definisjoner av ”grov kriminalitet” samt spesifikke lovbrudd som blir gjeldende som godkjente formål for datauthenting, de forskjellige spesifikke lovbrudd blant nasjonene synes også og i stor grad sammenfalle, da arbeid mot terrorisme, spionasje og barneporno er gjengangere.

2.5 Lagringstid

EU har valgt å gi statene en ramme på 6-24 måneders lagringstid, det er dermed opp til de forskjellige medlemsstatene å avgjøre hvor lenge data skal lagres. De aller fleste medlemsnasjoner har valgt å lagre data i 12 måneder. Sveits, Liechtenstein, Romania, Luxembourg og Kypros har valgt 6 måneder. Slovakia og Latvia lagrer i 18 måneder og Irland i 36 måneder (12 måneder lengre enn direktivet åpner for). Et mindretall har dermed valgt å lovfeste noe kortere lagringstid, flertallet har lagt seg på 12 måneder, et mindretall har valgt noe lengre lagringstid. Det er kun et fåtall av medlemsstater som ennå ikke har innført direktivet.

2.6 Hvordan kan data hentes ut og av hvem?

Det foreligger i direktivet ingen krav til at det skal foreligge domstolskontroll med utlevering av data. Derfor er det opp til statene å regulere hvordan utlevering skal foregå rent prosessuelt. Art. 9 i direktivet krever dog at statene må ha et uavhengig kontrollorgan som skal overvåke implementeringen og bruken av datalagringsdirektivet i de særskilte statene, slik jeg tolker ordlyden i art. 9 er det her ikke snakk om et organ som skal kontrollere konkrete saker, men derimot et organ som skal overvåke statistikk og gjøre kontroller av hvorfor, hvordan og når trafikkdata blir brukt rent overordnet.

I Danmark har de valgt en løsning der det i de aller fleste tilfeller kreves en kjennelse fra retten for å hente ut trafikkdata. Det samme har det store flertall av EU-stater valgt. Prosessen synes dermed i de fleste tilfeller å innebære en forespørsel fra politiet til en nasjonal domstol som behandler søknaden i henhold til nasjonale regler. En slik domstolskontroll er en sikkerhetsmekanisme som fungerer som en garanti mot vilkårlige inngrep fra politi- og påtalemyndigheter. Et unntak er Finland, der data utleveres på forespørsel fra politimyndighetene.

Når det gjelder hvem som skal få tilgang til data er det fra direktivets side opp til statene selv å velge hvilke offentlige myndigheter som skal ha mulighet til å hente ut data. I Norge er løsningen som er foreslått i høringsutkastet at kun politiet skal kunne begjære tingretten om

mulighet til å hente ut data, samtidig som høringsutkastet uttaler at det prinsipielt ikke er noe i veien med at også andre offentlige myndigheter som tollmyndigheter, skattemyndigheter og lignende får tilgang på data.

2.7 Sentralisert eller desentralisert lagring

Alle tilbydere av offentlig tilgjengelige kommunikasjonstjenester skal jf. direktivets artikkel 3, lagre trafikkdata. Direktivet regulerer ikke hvorvidt lagring skal foregå sentralisert[19] eller desentralisert[20]. De land jeg har sett nærmere på har alle valgt en desentralisert løsning. Begge disse løsninger har problematiske sider. Staten kan med en sentralisert løsning selv ivareta datasikkerhet, bygningssikkerhet, backup og gode tilgangsrutiner. Samtidig er det dog langt større konsekvenser om noen kommer seg forbi disse sikkerhetsforanstaltningene, da det komplette bildet fra hver bruker vil være lagret her. Som en motsetning er det kun fraksjoner av borgernes trafikkdata som ligger hos hver tilbyder, så en desentralisert løsning vil medføre mindre risiko for komplette lekkasjer av kommunikasjonshistorikk. På den annen side har dog mange lokale tilbydere færre midler til sikkerhet og dette vil nok påvirke graden av sikring mot ulovlig tilgang.

2.8 Om gjennomføringen i forskjellige medlemsstater

2.8.1 Innledning

Det er et bredt spekter av forskjellige gjennomføringsmodeller i Europa. Det er forskjeller på hvor lenge data blir lagret, hvilke data som lagres, hvordan data lagres, hvem som kan hente ut data, hvordan data kan hentes ut, samt mange andre større og mindre forskjeller. Det har krystallisert seg en en del momenter som lagringstid, prosessuelle regler for uthenting av data og en del andre viktige momenter hvor større grupper medlemsland har mye til felles. Jeg vil i dette kapittelet gå gjennom en del hovedtrekk ved gjennomføringsmodellene og på denne måten legge grunnlaget for vurderingen opp mot artikkel 8 i EMK. Jeg vil også i noen grad foregripe begivenhetene og knytte noen av drøftelsene opp mot EMK allerede her. Det er naturlig å avgrense min drøftelse til hva som lagres, hvem som lagrer, hvem som godkjenner uthenting og eventuelle kontrollorgan.

I dette kapittelet vil jeg også gå gjennom noen forskjellige gjennomføringsmodeller fra forskjellige EU-land. Hva er forskjellene og hva utgjør disse forskjellene i praksis? Jeg deler implementeringen inn i de forskjellige bestanddeler og vurderer de forskjellige modellene opp mot hverandre på de forskjellige punktene. De land jeg har valgt å gå nærmere gjennom i denne delen er Danmark, Finland, Nederland og Spania. Årsaken til at jeg har valgt nettopp

19 En statlig database der alle data lagres etter oversending fra de forskjellige tilbydere.
20 Lagring ute hos hver enkelt tilbyder

disse fire til en nærmere drøfting, er at de etter mitt syn representerer et geografisk og politisk tverrsnitt av medlemsstatene. Det vil i praksis være umulig å få en presis og perfekt gjennomsnittsgruppe av medlemsstater, da spennet i kultur, politikk, økonomi og andre felter er så stort. Jeg vil uansett likevel også peke på enkeltmomenter fra en del andre medlemsstater for å nyansere bildet og få et bredere inntrykk. I tillegg vil jeg avslutningsvis gå gjennom gjennomføringen i Romania og Tyskland, der forfatningsdomstoler har avvist implementeringen av direktivet. Årsaken til at jeg tar med disse to tilfellene, er at begge domstolene i stor grad lener mot EMD i sin argumentasjon og både problemstillinger og vurderingstema er parallelle.

2.8.2 Gjennomføring i Danmark, Finland, Spania og Nederland

2.8.2.1 Data nødvendig for å spore og identifisere kommunikasjonskilden

2.8.2.1.1 Fast- og mobiltelefoni

Her krever ordlyden i i direktivet at nummer, navn og adresse tilhørende den som ringer ut skal. Dette synes også å være gjennomgående hos de landene jeg har undersøkt. I Danmark lagres utgående nummer, navn og adresse på abonnent eller en registrert bruker.[21] Tilsvarende regler har man også i Finland[22] Nederland[23] og Spania[24]. Finland og Nederland er her marginalt forskjellig i det at EMS-tjenester nevnes eksplisitt.

2.8.2.1.2 Internettilgang, Internettepost og Internettelefoni

I Danmark skal følgende data lagres om en Internettøkts første og siste pakke i relasjon til avsender: Avsenders IP-adresse, transportprotokoll, avsenders portnummer, tidspunkt for øktens start og avslutning. I tillegg skal en sluttbrukers tildelte brukeridentitet lagres, brukeridentitet og telefonnummer som blir tildelt en kommunikasjonsøkt som inngår i et offentlig telefonnett. Navn og adresse på abonnent eller registrerte bruker hvis IP-adresse, brukeridentitet eller telefonnummer var tildelt på økt-tidspunktet samt øktens starttidspunkt og avslutningstidspunkt skal også lagres. Dette medfører et visst skille i graden av detaljinformasjon som blir lagret siden få andre land har valgt å lagre mottagerinformasjon for ordinær Internettrafikk. Når det gjelder lagring av port- og protokollinformasjon, kan dette i

21 Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) [Danmark]

22 Lag om dataskydd vid elektronisk kommunikation 16.6.2004-516 [Finland]

23 Bevoegd aftappen en toepassing van andere bevoegd- heden op grond van het wetboek van strafvordering en de wet op de inlichtingen- en veiligheidsdiensten 2002 in verband met telecommunicatie [Nederland]

24 Ley 25/2007, de 18 de octubre, de conservacion de datos relativos a las comunicaciones electronicas y a las redes publicas de comunicaciones [Spania]

stor grad brukes til å identifisere hva slags trafikk det er snakk om, man øker dermed graden av kartlegging. Man kan med denne informasjonen se om det er HTTP-trafikk, FTP-trafikk, epost-trafikk o.l. Dette medfører bl.a. at man kan se om jeg har overført filer, se om jeg har sendt epost, man kan se om jeg har brukt fildelingstjenester og en hel rekke andre ting. Dette kan dog omgås ved forholdsvis enkle grep.

2.8.2.2 Data nødvendig for å spore og identifisere kommunikasjonsmottager

2.8.2.2.1 Fast- og mobiltelefoni:

Når det gjelder mottager av kommunikasjon er reglene relativt like. I Danmark vil man måtte lagre navn, adresse til abonnent eller bruker, nummer som samtalen blir viderekoblet til og kvitteringer for mottatte meldinger. Dette er et regelverk som samsvarer med de andre landene jeg har undersøkt. Det er altså få og hovedsaklige språklige/semantiske forskjeller på hvordan denne delen av direktivet har blitt gjennomført. Den gjengse implementeringen ligger altså svært nær en ren oversettelse av direktivteksten.

2.8.2.2.2 Internettepost og Internettelefoni:

I forbindelse med Internettepost og Internettelefoni medfører implementeringen i Danmark at man ikke bare skal lagre data i forbindelse med epost og bredbåndstelefoni, men også at mottagerinformasjon for ordinær datatrafikk skal lagres. Mottagers IP-adresse, mottagers transportprotokoll og mottagers portnummer skal lagres for slik trafikk slik jeg har tolket det danske lovverket. I forhold til ordlyden i direktivet, er det noen faktorer som er verdt å merke seg her. For det første har de lovfestet logging av mottagers IP-adresse, portnummer og tjenesteprotokoll. Slik jeg tolker ordlyden i kapitteloverskriften ”concerning Internet e-mail and Internet telephony: the Internet service used;”, kan jeg ikke anse at dette skal gjelde all Internettbruk, kun bruken av epost og telefoni over Internett. Danmark er alene i å kreve lagring av mottagerdata på denne måten (blant de landene jeg har undersøkt), og stiller sådan i en særstilling også her. Nederland lagrer også til en viss grad data på mottager, men ikke i så stor grad som Danmark. Hos de andre landene er det kun trafikk i forbindelse med Internettelefoni og Internettepost som blir lagret. Spania har valgt å være mer tro mot ordlyden i direktivet og pålegger lagring av navn og adresse på abonnent knyttet opp mot en IP-adresse eller et telefonnummer.[25] Spania er sådan langt mer tro mot ordlyden i direktivet i artikkel 5, b, 2 enn det Danmark er. Det er naturlig å se på overskriftene i direktivets 5, b, 2 sammenholdt med 5, a, 2. Den sistnevnte har denne overskriften: ”concerning Internet access, Internet e-mail and Internet telephony:”, den førstnevnte har ordlyden ”concerning Internet e-mail and Internet telephony:”. En naturlig tolkning av disse to overskriftene innebærer at det i

25 Spania har valgt å følge ordlyden fra direktivet, og dermed ikke inkludert mottagerinfo for ordinær Internettrafikk.

forhold til 5, b, 2 ikke skal lagres trafikkdata for mottager for ordinær Internettrafikk. At Danmark likevel har valgt å implementere en løsning der slike data lagres viser at direktivet har blitt tolket forskjellig av forskjellige medlemsland og ført til merkbare forskjeller selv der slike forskjeller ikke har vært intensjonen.

2.8.2.3 Data nødvendig for å identifisere dato, tid og kommunikasjonslengde.

2.8.2.3.1 Fast- og mobiltelefoni:

I Danmark skal tidspunkt for samtalens start og avslutning lagres, dette gjelder for både fast- og mobiltelefoni. I tillegg skal tidspunkt for førstegangsaktivering av kontantkort lagres. Dette er i tråd med ordlyden i direktivet og det er heller ikke stor spredning blant implementeringene jeg har sett på dette området.

2.8.2.3.2 Internettilgang, Internettepost og Internettelefoni.

I forhold til Internettrafikk er det i Danmark slik at øktens starttidspunkt og avslutningstidspunkt skal lagres. Dette er, som flere andre momenter, relativt direkte oversatt fra direktivteksten. Det er kun semantiske forskjeller på dette området også, i forhold til de andre landene jeg har undersøkt.

2.8.2.4 Data nødvendig for å identifisere kommunikasjonstype

2.8.2.4.1 Fast- og mobiltelefoni

I Danmark blir det ikke eksplisitt omtalt hvilke data som skal lagres i forbindelse med identifikasjon av kommunikasjonstype i relasjon til fast- og mobiltelefoni. Ser man derimot på Nederland skal det lagres data som kan identifisere tjeneste brukt, det vil si for eksempel SMS, EMS eller MMS. Dette for å identifisere hvorvidt det er sendt multimediainnhold, ren tekst eller andre former for tjenester. Det samme synes å gjelde for Spania og Finland. Her er det i utgangspunktet et skille mellom Danmark og de andre landene jeg ser på.

2.8.2.4.2 Internettepost og Internettelefoni

Det danske regelverket påbyr lagring av port- og protokollinformasjon. Dette synes i stor grad å samsvare med de øvrige land jeg har sett på. Dette gjør at det er mulig å se hvilken type trafikk brukerne har benyttet seg av. Det være seg epost, FTP, SSH, IRC eller andre protokoller.[26]

26 FTP er en filoverføringsprotokoll som brukes for å sende/motta filer. SSH er en kryptert kommunikasjonsform mellom maskiner, IRC er en textkommunikasjonsprotokoll

2.8.2.5 Data nødvendig for å identifisere kommunikasjonsutstyr

2.8.2.5.1 Fast- og mobiltelefoni

I Danmark har man valgt å lagre IMSI- og IMEI-nummer, plassering av de master mobiltelefonen er koblet opp mot og celleinfo. I tillegg skal geografiske data i forbindelse med førstegangsaktivering av simkort lagres. Dette er i all hovedsak parallelt med ordlyden i direktivet og sammenfaller også med den implementeringen man finner i andre land.

2.8.2.5.2 Internettilgang, Internettepost og Internettelefoni

For Internettilgang, Internettepost og Internettelefoni har Danmark valgt og ikke eksplisitt ta dette med i lovgivningen, dette i motsetning til f.eks. Spania, der det fremgår at det når det gjelder Internettkommunikasjon skal telefonnummer i fall analog oppkobling lagres og for DSL skal informasjon om påkoblingsnode lagres.

2.8.2.6 Lokasjonsdata for mobiltelefoni

I Danmark har man valgt å lagre de geografiske celler mobiltelefonen er forbundet med ved kommunikasjonens start og avslutning samt de tilhørende masters presise geografiske plassering på tidspunkt for samtalens start og avslutning. Dette samsvarer i all hovedsak med ordlyden i direktivet, dette er også den løsningen som synes å være vanligst blant de landene jeg har undersøkt. Celleinfo og informasjon om de forskjellige masters plassering er gjennomgående, og dette er også tilstrekkelig for å sikre presisjon når man skal spore mobiltelefonsamtaler rent geografisk.

2.8.3 Uthenting av lagrede data

Det er forholdsvis store sprik i reglene for uthenting av data i de forskjellige medlemslandene. Jeg vil ta utgangspunkt i de danske reglene først. Ser man på Rettsplejeloven §§ 781, 782, 783 og 784, er det flere regler forbundet med uthenting av lagrede data.[27] For det første er det et krav at det foreligger konkret grunn til å tro at kommunikasjonsdataene som ønskes uthentet stammer fra kommunikasjon fra eller til en mistenkt. Datauthentingen må også antas å være av avgjørende betydning for etterforskningen. Videre er det et krav at etterforskningen gjelder et lovbrudd som har en strafferamme på minst 6 år, er en overtredelse av straffelovens kapittel 12 eller 13, eller en overtredelse av øvrige bestemte straffebud i bl.a. straffeloven og utlendingsloven. I § 782 finner man en proposrjonalitetsregel som også er en skranke mot misbruk og minsker sjansene for vilkårlige inngrep. Det er ikke mulighet å gripe inn i meddelelseshemmeligheten hvis uthentingen er uforholdsmessig. Av § 783 fremgår det at uthenting av data kun kan skje etter rettens kjennelse. Her skiller Danmark seg markant fra bl.a.Finland, som ikke har rettslig kontroll med uthenting av lagrede data.

27 LBK nr 1053 af 29/10/2009 - Bekendtgørelse af lov om rettens pleje

Det er også verdt å nevne at det i Danmark utnevnes en advokat for de som blir utsatt for overvåkning og/eller uthenting av data, noe som gir de som blir utsatt for denne typen inngrep mer rettsikkerhet. Her er det både likheter og forskjeller sammenlignet med de andre europeiske land. Som nevnt over er det ikke i Finland et krav om rettslig kontroll med uthenting av data, mistenkte får ei heller oppnevnt advokat i denne prosessen. I Finland er det derimot et krav om strafferamme på minst 4 år, med unntak for nærmere presiserte kategorier av lovbrudd. Slik jeg ser det er den manglende juridiske kontrollen en svakhet ved det finske systemet. Det nederlandske systemet har også et lignende system der både dommere, aktor, lederskikkelser innad hos påtalemyndigheten samt ledere i den militære og sivile etterretningstjenesten kan godkjenne uthenting av data. Slik jeg tolker implementeringen i Nederland vil man dermed ende opp på et midtpunkt mellom Finland som et ytterpunkt der politiet selv kan hente ut data og f.eks. Spania, der det er flere sikkerhetsmekanismer for å unngå misbruk av lagrede data. Det fremgår av lovgivningen i Spania at det ikke bare er krav om rettslig kontroll med uthenting av data, men at det kun er en isolert gruppe som har myndighet til å søke om uthenting av dat. Slik får man dermed to lag med kontroll av legitimitet av krav om uthenting. Det at man i Danmark har en proposjonalitetsterskel fortjener også en liten utdypning. Dette gjør at man ved den rettslige kontrollen alltid må ha i bakhodet at inngrepet ikke skal stå i et misforhold til den nytte man kan få. Har eventuelle data uansett lav bevisverdi eller har politiet ikke klart å fremheve at dette vil være sentrale bevis, er det lite sannsynlig at slike data vil bli tillatt hentet ut slik ordlyden fremstår.

Noen av løsningene en del medlemsstater har valgt, kan fremstå som problematiske i relasjon til en harmonisering av EMK og direktivet. Jeg vil avslutningsvis se litt nærmere på noen av disse. Først i rekken er praksis for uthenting av data.

Direktivteksten selv definerer ikke "serious crime", vilkåret for uthenting av lagrede data, ytterligere, og man har ei heller uttalelser fra forarbeidene som kan bidra til tolkningen her. Dette har ført til en rekke forskjellige mønstre. Tyskland, Belgia og Kypros innførte i sitt regelverk en grense der kun lovbrudd med strafferamme over fem år kan hjemle uthenting av data.[28] Nederland og Frankrike har derimot en tilsvarende grense på ett år. På et annet plan har man Tsjekkia, Estland, Polen og Malta. Disse landene har valgt å legge definisjonen av "serious crime" opp til sine nasjonal domstoler, slik at den til enhver tid fungerende dommer kan definere dette. Dette kan være problematisk da det skaper usikkerhet rundt hva som faktisk kan defineres som "serious crime". Dette gjør situasjonen mindre forutberegnelig for borgerne. Selv om man etter hvert skulle få nasjonale paradigmer basert på rettspraksis, vil det likevel være vanskelig å skape uttømmende regler gjennom rettspraksis, noe som vil skape usikkerhet for borgerne. Det vil dermed være vanskelig å forutse når ens trafikkdata kan/vil bli utlevert.

Et annet forhold som også blir nevnt i den ikke publiserte evalueringsrapporten fra EU, er at flere medlemsland har valgt å gjennomføre et lovverk som går utover det direktivet påbyr.[29] Lagrede data kan sådan ikke bare brukes til "serious crime", men også til å omfatte f.eks.

28 Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communications

åndsverksrelaterte søksmål (Storbritannia). Andre medlemsstater har også valgt å ta med andre områder som f.eks. savnede personer-søk, kapitalmarkedsovervåkning o.l. Det at medlemsstatene har valgt å tolke direktivet utvidende er problematisk. Slik jeg tolker direktivets ordlyd, er det på de fleste punkter et minimumsdirektiv (lagringstid er et av unntakene her), slik er det i utgangspunktet åpent for at land kan både lagre flere typer data og at data kan brukes til andre formål. Problemet med denne praksisen er at den demokratiske prosessen ikke i forkant har tatt høyde for denne typen bruk når det gjelder proporsjonalitet og nødvendighet. Vurderinger av denne typen vil kunne ha andre resultater enn når det gjelder forebygging og etterforskning av grov kriminalitet.

2.8.4 Lagringstid

Alle de land jeg har sett nærmere på har lagt seg på 12 måneders lagringstid. Dette er i det store og hele normen de fleste land i Europa legger seg på og også gjennomsnittslagringstiden.[30] Man har noen få land som ligger på 6 måneder, og noen andre som ligger på 24 måneder. (Samt et land som ligger på 36 måneder, og sådan bryter med maksgrensen i direktivet). At man så ofte har havnet på et midtpunkt i forhold til spennet i direktivteksten gjenspeiler nok kampen mellom politimyndigheter og andre som ønsker så lang lagringstid som mulig og datatilsyns interesse i å beskytte borgernes kommunikasjonsdata og dermed kutte ned lagringstiden så mye som mulig.

Det fremgår i en ikke ennå offentlig publisert rapport at det ikke foreligger objektive data som forklarer det store spennet i valg av lagringstid hos de individuelle medlemsstatene.[31] Jeg vil dermed ikke prøve å gå nærmere inn på mulige årsaker utover den foran nevnte interesseavveiningen. Det at vi i Norge har innstilt på 6 måneders lagringstid i høringsutkastet høringsdokumenter fra myndighetene, kan indikere sådan muligens at datatilsynet og de verdier de forfekter står sterkere enn i deler av Europa i forhold til påtalemyndigheter og politi.[32] (I lovforslaget som kom rett før jul har regjeringen foreslått en lagringstid på 12 måneder, og går dermed bort fra dette).

2.9 Dommer fra Tyskland og Romania

2.9.1 Innledning

Jeg har valgt å ta med to nasjonale forfatningsdommer som begge avviser den implementeringer av direktivet de lovgivende forsamlinger har vedtatt. Årsaken til at jeg har

29 Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communications s. 5

30 Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communications s. 6

31 Room Document - Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communications

32 http://www.regjeringen.no/nb/dep/sd/dok/hoeringer/hoeringsdok/2010/horing---datalagring.html?id=590001

med disse dommene i oppgaven, er at de begge, synes å legge seg tett opp mot den argumentasjon EMD tradisjonelt har brukt i saker som omhandler EMK art. 8. Begge stater har grunnlovsregler som samsvarer sterkt med EMK art. 8. Både problemstillinger og vurderingstema synes sådan å samsvare med praksis fra EMD på dette området. Domstolene viser direkte til utsagn fra EMD og inkorporerer sågar disse i sine resonnementer. En forfatningsdomstolsdom fra Tyskland er i seg selv ikke en rettskilde som med særlig tyngde kan anføres i drøftelser om EMK. Samtidig synes jeg det er verdt å trekke inn både denne dommen og dommen fra Romania, da begge baserer seg på lovtekster som i stor grad er sammenfallende med EMK art. 8 og begge lener seg på både implisitte og eksplisitte henvisninger til EMDs praksis. Man kan anse disse dommene for å være uoffisielle generalprøver for en eventuell prøving for EMD. Dette er en analogi med åpenbare svakheter, men jeg anser årsakene nevnt over for å være tungveiende nok til å ta disse med i oppgaven. Jeg vil også trekke noen linjer til andre gjennomføringsmodeller i denne delen av oppgaven.

2.9.2 Tyskland

Tyskland innførte datalagringsdirektivet i 2007 .[33] Det ble (både før implementeringen, men desto mer etter dette tidspunktet) utøvd utstrakt motstand mot innføringen både fra politiske partier i opposisjon og organisasjoner i Tyskland. En sak ble etter hvert reist for den nasjonale forfatningsdomstolen.[34]

I Tyskland valgte de en gjennomføringsmodell med 6 måneders lagring, rettskjennelser for direkte uthenting av data, ingen rettskjennelse for indirekte uthenting og bruk av data (der politiet sitter med en IP-adresse og vil ha ut kundeinformasjon, ikke uthenting av datamengde fra en gitt celle til et gitt tidspunkt). Når det gjelder hva som skulle lagres, la den tyske loven seg i all hovedsak på en nærmest ordrett oversettelse av direktivteksten. I det følgende vil jeg prøve å belyse sentrale deler av den tyske domstolens argumentasjon. Spesielt der domstolen knytter sine resonnementer opp mot EMK har jeg valgt å bruke litt tid.

I sin dom uttaler den tyske forfatningsdomstolen først at ubetinget lagring av all data ikke nødvendigvis i seg selv er ikke-konstitusjonell, men at den tyske grunnloven stiller særlige krav til gjennomføringen. Spesifikt var det artikkel 10 i den tyske basisloven (grunnloven) som var rettsgrunnlaget. Denne artikkelen er til forveksling lik artikkel 8 i EMK.[35] I tysk rettspraksis har man i tillegg utviklet en lære om lovkvalitet, legitime mål og proporsjonalitet som også ligner den tilsvarende læren fra EMD.[36] Dette bidrar til å forsterke likhetene med

33 Telekommunikationsgesetz §§113a und 113b. [Tyskland]

34 The Arbeitskreis Vorratsdatenspeicherung er her verdt å nevne, en tverrpolitisk organisasjon.

35 Article 10 [Privacy of correspondence, posts and telecommunications]
(1) The privacy of correspondence, posts and telecommunications shall be inviolable.
(2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.

praksis fra EMD og er en av hovedårsakene til at jeg anser dommen som relevant for oppgaven.

Retten kommer i sitt infoskriv om dommen først med en del generelle kommentarer til allmenn lagring av data og de konsekvenser det kan ha. Retten går også lengre enn både EU og andre, nasjonale politiske instanser i å beskrive direktivet i et kritisk lys.[37] Domstolen sier i sitt presseskriv følgende:

> ”Even though the storage does not extend to the contents of the communications, these data may be used to draw content-related conclusions that extend into the users’ private sphere. In combination, the recipients, dates, time and place of telephone conversations, if they are observed over a long period of time, permit detailed information to be obtained on social or political affiliations and on personal preferences, inclinations and weaknesses. Depending on the use of the telecommunication, such storage can make it possible to create meaningful personality profiles of virtually all citizens and track their movements. It also increases the risk of citizens to be exposed to further investigations without themselves having given occasion for this. In addition, the possibilities of abuse that are associated with such a collection of data aggravate its burdensome effect. In particular since the storage and use of data are not noticed, the storage of telecommunications traffic data without occasion is capable of creating a diffusely threatening feeling of being watched which can impair a free exercise of fundamental rights in many areas.”

Den tyske domstolen setter her søkelyset på potensielle negative følger av direktivet. Konsekvensene belyses og konkretiseres.

Etter en generell innføring i ulemper ved og muligheter med direktivet, går retten videre med en mer spesifikk analyse av hvor problemene med den nåværende tyske implementering foreligger. Det er fire hovedområder forfatningsdomstolen legger spesiell vekt på. Datasikkerhet, gjennomsiktighet rundt datalagring, rettssikkerhet rundt lagring/uthenting og graden av presisjon i lovverk rundt hvilke forbrytelser som hjemler uthenting av data. Slik jeg tolker dommen, argumenterer den tyske domstolen for alle disse momentene under en paraply av proporsjonalitet.

Jeg vil først se på problemstillinger rundt datasikkerhet. I denne forbindelse definerer jeg datasikkerhet som både programvare- og maskinvareløsninger som minsker faren for ulovlig tilgang til lagrede data. Så langt i mine undersøkelser av implementering av datalagringsdirektivet i forskjellige medlemsland, har jeg ikke funnet noen gjennomføringsmodeller som regulerer datasikkerhetsproblematikk i detalj. Mange gjør som den tyske loven, legger en generell kvalitetsstandard til grunn i lovverket, uten å konkretisere dette i form av spesifikke retningslinjer verken i lovs form eller forskrifter.

36 De Vries, 2010, http://vub.academia.edu/KatjadeVries/Papers/176961/German_Constitutional_Court_Judgment_on_Data_Retention_Goodbye_Unlimited_Surveillance_Hello_Proportionality

37 Bundesverfassungsgericht, 2010, http://www.bundesverfassungsgericht.de/en/press/bvg10-011en.html

Forfatningsdomstolen anser ikke dette for å være tilstrekkelig for å sikre mot misbruk av data. Den påpeker at man bør innføre spesifikke og strenge krav til datasikkerhet i forbindelse med lagring av trafikkdata. Dette for å sikre borgerne mot ulovlig tilgang og dermed gjøre lagringen mindre inngripende. Sikkerhetsmekanismer som hindrer lekkasjer, vilkårlige inngrep og misbruk vil alle bidra til at et inngrep fremstår som mindre alvorlig. Dette er slik jeg tolker det også sammenfallende med praksis fra EMD. I Malone-saken fremgår det at nasjonale lover som regulerer inngrep, må gi tilstrekkelig beskyttelse mot vilkårlige inngrep fra myndighetene.[38] Malone-dommen er en av dommene jeg vil vise mest til i denne oppgaven, så jeg vil kort gjøre rede for hva saken gjaldt. Malone-saken omhandlet uthenting og bruk av "meteringdata" i Storbritannia.[39] Hovedvekten av dommen dreier seg om lovkvalitetsspørsmål, men andre forhold i relasjon til overvåkning av forskjellig art blir også drøftet. En av grunnene til at jeg har valgt å bruke Malone-dommen er at den bl.a. omhandler trafikkdata, og ikke innholdssdata. Dette gjør den særlig relevant for min problemstilling. Slik jeg tolker Malone-dommen, stiller EMD krav til nasjonal lovgivning utover det at lovgivningen skal være tilgjengelig og presis. Lovgivningen må også i tilstrekkelig grad sikre borgerne mot misbruk når overvåkingstiltak blir iverksatt. Slik den tyske retten ser det kan man godt delegere ansvaret for detaljgjennomføring og tekniske løsninger til en komité eller en undergruppe under statlig kontroll. Det viktigste synes å være at det er klare og strenge krav til datasikkerhet. Misbruk av data og lekkasjer er for mange det mest åpenbare problemet med direktivet, og mangelen på gode og godt utarbeidede sikkerhetsløsninger er en akilleshæl for direktivet etter min mening. Slik jeg har tolket rettspraksis kan dette omfatte både teknisk infrastruktur, uthentingsrutiner, programvareløsninger og rent fysisk bygningskontroll/tilgangskontroll, uten at jeg anser det som sannsynlig at EMD vil legge seg på et så detaljert nivå. På denne måten kan man i stor grad eliminere misbruk fra ansatte hos telekomtilbydere, fra politiets side og fra eksterne kriminelle elementer som vil misbruke lagrede data.

Det neste hovedpunktet fra forfatningsdomstolen er at det ikke var tilstrekkelig gjennomsiktighet rundt uthenting av data. Her fremgår det at domstolen vil avvise et prinsipp der uthenting av data skal hemmeligholdes og fremholder at de det gjelder må informeres om datauthenting såfremt ”otherwise the purpose of the investigation served by the retrieval of data would be frustrated”. Denne løsningen vil i praksis snu bevisbyrden og pålegge politiet en plikt til å vise at hemmelighold er nødvendig. Slik jeg tolker den tyske domstolen, sier de her at et inngrep av denne art er mer nærliggende å akseptere om gode sikkerhetsmekanismer er på plass. Dette er en tradisjonell proporsjonalitetsvurdering. Igjen er parallellen til Malone-dommen etter mitt syn klar. Der fremgår det at skjønnsmessig makt utført i hemmelighet, utgjør en risiko for vilkårlighet.

Rettens tredje hovedmoment er at det er en mangel på presisjon når det gjelder hvilke lovbrudd som kan hjemle uthenting av data. For det første synes det å være relativt bredt definert hvilke lovbrudd som kan hjemle uthenting av data i utgangspunktet. I tillegg kan alle

38 Malone v. The United Kingdom - 8691/79 (1984)

39 Televerkets data knyttet til bruk av et telefonabonnement, rudimentære trafikkdata

lovbrudd relatert til telekommunikasjonsutstyr hjemle uthenting av data. Tyskland åpner slik for et mer vidtrekkende bruksområde for trafikkdata enn direktivet i utgangspunktet krever, domstolen sier bl.a.:

> ”Here, the legislature no longer confines itself to the use of data to prosecute serious criminal offences, but goes far beyond this, and thus far beyond the objective of data storage specified by EU law”[40]

Det fremgår av dommens avsnitt om mangel på presisjon at domstolen ønsker lovgivning der det fremgår på en presis og forståelig måte hva som kan hjemle uthenting av trafikkdata i forbindelse med etterforskning av kriminelle handlinger, samt uthenting i forbindelse med avverging av fare og bruk innad i etterretningstjenestene. Denne presisjonen gjør det enklere for borgerne å forutse sin rettsposisjon og er sådan både relatert til lovkvalitet og proporsjonalitet. Det kan synes som at den tyske domstolen legger til grunn at det er enklere å godta et inngrep, om det er klare rammer for når inngrepet kan skje. De argumentene den tyske domstolen bruker, er her tildels analoge med uttalelser i bl.a. Malone-saken. Slik jeg tolker praksis fra EMD, er presise og forutberegnelige lover er en av flere forutsetninger for at en nasjonal gjennomføringsmodell skal kunne harmoniseres med EMK art. 8. Dette blir drøftet mer inngående senere i oppgaven.

Avslutningsvis i denne delen av drøftelsen fremholder også retten at det er en hel rekke grupperinger som må falle helt utenfor uthentingsmuligheter. Det være seg kommunikasjon med psykolog, helsetjenester o.l. over telefon/epost. Domstolen fremhever at slike tjenester må unndras uthenting hvis loven skal kunne anses for å være proporsjonal. Jeg har til gode å se at dette er noe nasjonale innføringsregimer tar høyde for. At ingen land jeg har undersøkt har spesifisert dette konkret i sin gjennomføring er en svakhet med gjennomføringen etter mitt syn. Samtidig kan det være verdt å merke seg at denne typen regulering kan være vanskelig å gjennomføre. Hva skal man gjøre med kommunikasjon en advokat mottar på privattelefonen? Hva om en advokat jobber hjemmefra med sensitive dokumenter angående klienter og sender disse på sin private epost? Det kan synes som at forhåndssensur av lagring kan fremstå som umulig. Det kan derfor være naturlig å anbefale sensur ved uthenting av data. Dette kan gjøres i en utleveringsprosess, noe som vil ivareta deler av vernet disse grupperingene bør ha. Når det gjelder uthenting av data for avverging av fare og til bruk i etterretningstjenesten, konkluderer retten forholdsvis raskt med at de vide fullmakter som her gis ikke er tilstrekkelig presise. De vide fullmaktene gjør det mulig for politi og etterretningsvesen å hente ut data for nærmest all sin virksomhet. Dette aviser forfatningsdomstolen som grunnlovsstridig uten å gå særlig dypt inn i materien. Her fremgår det igjen at spesifikke forbrytelser må ligge til grunn for uthenting av data, uansett formål. Det er her også mange paralleller til de vurderingene EMD tradisjonelt gjør i forbindelse med artikkel 8-saker. Det kan være naturlig å peke på Malone-saken der EMD gjør lignende vurderinger:[41]

40 Federal Constitutional Court - Press office -
Press release no. 11/2010 of 2 March 2010
41Malone v. The United Kingdom - 8691/79 (1984)

> "The issue to be determined is therefore whether, under domestic law, the essential elements of the power to intercept communications were laid down with reasonabler presicion in accesssible legal rules that sufficiently indicated the scope and manner of exercise of the discretion conferred on the relevant authorities"

Den tyske domstolen legger seg, både når det gjelder dette avsnittet og det forrige på linje med de drøftelsene EMD har lagt til grunn på lignende områder. Argumentasjonen er parallell.

Det fjerde momentet omhandler rettssikkerhet i forbindelse med uthenting av data. Her understreker domstolen behovet for domstolsbehandling ved utlevering av data. Videre at det må foreligge sanksjoner når det foreligger misbruk av retten til uthenting. Når det gjelder domstolskontroll det i det øvrige Europa varierer implementeringsteknikker. Selv om de fleste statene har innført en eller annen form for rettslig kontroll, er det også andre stater der data utleveres direkte til politiet etter forespørsel. Slik jeg tolker den ovennevnte praksis fra EMD, er rettslig kontroll med uthenting en grunnleggende forutsetning for at generell lagring av trafikkdata skal være i samsvar med EMK. Uten en slik kontroll er faren for misbruk for stor. Uten rettslig kontroll og en eventuell varsel til borgerne om at overvåkning skjer, vil, slik den tyske forfatningsdomstolen kommer inn på, trusselen om overvåkning ligge som en latent trussel i relasjon til all kommunikasjon over telefon og Internett.

Den tyske dommen drøfter flere relevante vurderingstema og problemstillinger. Den tar opp sider ved innføringen i Tyskland som også går igjen i andre medlemsland. Den argumentasjonen domstolen fører ligger også tett opp til de vurderinger EMK tradisjonelt har tatt samtidig som den også eksplisitt viser til EMK. Jeg tror dette kan være en god indikator på hvilke vurderinger EMD med sannsynlighet vil gjøre. Man kan selvsagt ikke dra noen direkte paralleller mellom resonnementene den tyske domstolen gjør og hva som mest sannsynlig vil utgjøre EMDs praksis, men samtidig er det tydelig at den tyske domstolen har støttet seg på praksis fra EMD i sine vurderinger.

2.9.3 Romania

Datalagringsdirektivet ble innført ved lov no.298/2008 i Romania i 2008.[42] Implementeringen er med få unntak i tråd med ordlyden i direktivteksten. Romania er et av få land (av de jeg har undersøkt), som har eksplisitte regler om datasikkerhet i sitt implementeringslovverk. Datasikkerhet blir dog ikke tatt opp som problemstilling i dommen, så jeg vil ikke gå nærmere inn på det her. Romania er også et av få land som har valgt å lovfeste prosedyrer for å evaluere innføringen. Jeg kan helt kort nevne at lagringstid i denne innføringsmodellen var

42 Law no.298/2008 regarding the retention of the data generated or processed by the public electronic communications service providers or public network providers, as well as for the modification of law 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area [Romenia]

seks måneder. Dette er under gjennomsnittslagringstiden på tolv måneder ellers i Europa. Jeg vil ikke gå nærmere inn på gjennomføringsmodellen Romania har valgt siden lite skiller seg fra en ren oversettelse av direktivet. Jeg vil derimot bruke litt tid på forfatningsdommen som veltet innføringsloven. Den rumenske dommen går lengre enn den tyske dommen i å legge seg på samme linje som EMK art. 8. Dommen siterer EMK og viser til flere sentrale dommer om overvåkning fra EMK.

Datalagringsdirektivets implementering i Romania ble avvist i dom no.1258 i den Rumenske forfatningsdomstol den 8. oktober 2009.[43] Det er i hovedsak to hovedmomenter den rumenske forfatningsdomstolen legger avgjørende vekt på i dommen. Det første er sammenfallende med et av momentene i den tyske dommen; presisjon. Det andre poenget domstolen løfter frem, er at en lov om allmenn lagring av trafikkdata vil uthule den grunnlovsfestede retten til respekt for korrespondanse og privatliv. Begge disse momentene synes å bli drøftet i forhold til proporsjonalitet og nødvendighet.

Det rettslige grunnlaget er den rumenske konstitusjonens artikkel 53. Ordlyden i denne bestemmelsen er i stor grad sammenfallende med EMK art. 8.[44] Jeg skal i det følgende redegjøre for mitt syn på dommen og hvordan den relaterer seg til EMD-praksis.

Den første problemstillingen forfatningsdomstolen angriper, er spørsmålet om presisjon. Dette er altså et problem begge de nasjonale domstolene tar opp. Domstolen legger vekt på at både selve definisjonen av hvilke data som skal lagres og hvordan de skal brukes gir rom for utstrakt tolkning. I artikkel 1, paragraf 2 av loven, blir hvilke data som skal lagres definert. Som et utgangspunkt er det nærmest en ordrett oversettelse av direktivteksten. I tillegg kan "the related data necessary" også utleveres. Den rumenske domstolen anser dette for å være en for vidtrekkende skjønnskompetanse. "The related data necessary"åpner for en vid definisjon av hva som skal lagres og utleveres. Den rumenske domstolen viser til Rotaru-dommen og bruker sitater fra denne dommen i sitt resonnement.[45] Tilsvarende bruker dommen aktivt sitater fra Sunday Times-dommen.[46] Hovedpoenget synes her å være at lovhjemmelen for lagring bør gjøres så presis som praktisk mulig. Her blir ikke ”the related data necessary” tilstrekelig presist. Man gir i realiteten myndighetene mulighet til å utvide området for data

43 DECISION no.1258 (1) from 8 October 2009

44 ARTICLE 53

(1) The exercise of certain rights or freedoms may only be restricted by law, and only if necessary, as the case may be, for: the defence of national security, of public order, health, or morals, of the citizens' rights and freedoms; conducting a criminal investigation; preventing the consequences of a natural calamity, disaster, or an extremely severe catastrophe.

(2) Such restriction shall only be ordered if necessary in a democratic society. The measure shall be proportional to the situation having caused it, applied without discrimination, and without infringing on the existence of such right or freedom.

45 CASE OF ROTARU v. ROMANIA (Application no. 28341/95)

46 The Sunday Times v United Kingdom (Series A No 30), European Court of Human Rights (1979-80) 2 EHRR 245, 26 APRIL 1979

som skal omfattes av lagringsplikten, og dermed blir muligheten for forutberegnelighet liten. En lignende kritikk blir reist mot uttrykket "threats to national security" i artikkel 20 av loven. Denne bestemmelsen hjemler uthenting av trafikkdata i forbindelse med saker som truer rikets sikkerhet. Bestemmelsen definerer ikke dette nærmere og har ingen strafferammeterskel. Domstolens syn er at dette er et kriterium som ikke kan anses for å være presist nok, og at borgerne dermed ikke har tilstrekkelig informasjon til å avpasse sin adferd.

> "The legislativ [sic] does not define what "threats to national security" mean, so that, with the lack of precise criteria, some regular, routine actions of the physical and legal persons may be appreciated, in an arbitrary and abusive way, as such threats."[47]

Her fremgår det tydelig at domstolen frykter vilkårlig misbruk av skjønnsrommet myndighetene vil få ved innføring av en slik bestemmelse.

Denne første problemstillingen belyser i likhet med dommen fra Tyskland behovet for en så presis og konkret lovgivning som mulig på dette området. Lovgivningen må skape forutberegnelighet og klare grenser på et område der konsekvensene ved misbruk er store.

Det andre og mer prinsipielle problemet med implementeringen, er at retten anser den nye lovgivningen for å undergrave hele hovedregelen om respekt for privat kommunikasjon. Hovedregelen både nasjonalt i Romania og i EMK er at respekt for privatliv og korrespondanse skal foreligge, og at unntak kun skal skje jf. de vilkår man bl.a. finner i EMK 8 (som domstolen henviser til). Den rumenske domstolen sier dette:

> “The obligation to retain the data, established by Law 298/2008, as an exception or a derogation from the principle of personal data protection and their confidentiality, empties, through its nature, length and application domain, the content of this principle, as it was guaranteed by law 677/2001 and law 506/2004. [...] The legal obligation that foresees the continuous retention of personal data transforms though the exception from the principle of effective protection of privacy right and freedom of expression, into an absolute rule. The right appears as being regulated in a negative manner, its positive role losing its prevailing role.”

Her fremgår det at domstolen anser innføringsloven for å være en uthuling av prinsippet om rett til respekt for privatliv og korrespondanse. Her går domstolen langt i å diskvalifisere enhver innføring av direktivet som medfører allmenn lagring. Det kan bli interessant å følge utviklingen i Romania videre. Dette kan indikere at forfatningsdomstolen ønsker en grunnlovsendring før direktivet kan innføres for å sikre demokratisk kontroll. Domstolen stiller seg spørsmålet: I hvor stor grad kan man si at et prinsipp om ikke-overvåkning er en reell hovedregel og at privatlivet blir beskyttet når utgangspunktet er allmenn overvåkning? Her setter den rumenske domstolen søkelyset på noe som på mange måter kan anses å være et

47 http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

paradigmeskifte i den europeiske rettstenkningen. Der man nå i flere tiår har hatt et veldig stort fokus på personvern, databeskyttelse og regelverk som beskytter korrespondanse og privatliv, ser det nå ut som man går mot et system der det i større grad er aksept for å gripe inn i disse rettighetene for å bekjempe forskjellige former for kriminalitet. Datalagringsdirektivet er bare ett eksempel på dette, også ACTA (ACTA Anti-Counterfeiting Trade Agreement), som er et verdensomspennende traktatverk, viser at de krefter som ønsker større grad av overvåkning har fått større gjennomslagskraft. Dette både på bakgrunn av grov kriminalitet og terrorisme, men man ser også at markedskreftene og da spesielt opphavsrett-relaterte bransjer, støtter gjennomføringen av slike tiltak.

2.9.4 Oppsummering

Som tidligere nevnt, er det begrenset hvor langt man kan dra analogien om disse dommene som en generalprøve for en eventuell prøving for EMD. Likevel er det verdt å merke seg de parallelle problemstillingene, de like vurderingstemaene og måten begge domstolene legger sin argumentasjon tett opp mot praksis fra EMD og de facto inkorporerer sitater fra EMD i sine resonnementer.

Begge dommene synes å legge vekt på presisjon som et problem. Presisjon i forbindelse med hva som skal lagres og presisjon i forbindelse med når uthenting kan skje. I tillegg belyser begge dommene manglende eller mangelfull regulering av mekanismer som skal hindre misbruk og vilkårlige inngrep. Dette er momenter jeg vil ta med meg videre i oppgaven.

3 Trafikkdatas verdi som etterforskningsverktøy

En sentral forutsetning for å kunne foreta en proporsjonalitetsvurdering i forhold til bruken av trafikkdata, er kjennskap til hvordan disse data brukes, hvor effektive de er og hva mulige konsekvenser kan bli av ikke å ha dem. I dette kapittelet skal jeg gå gjennom data fra Danmark, Tyskland, Sverige og Norge. Et sitat fra en svensk utredning belyser viktigheten av presis og god informasjon:

> ”Det är av grundläggande betydelse i en rättsstat att rätten till skydd för privat- och familjeliv respekteras. För en effektiv brottsbekämpning är det dock nödvändigt att det finns tillräckliga befogenheter för de brottsbekämpande myndigheterna att i vissa väl avgränsade fall kunna använda hemliga tvångsmedel.
>
> Vid avvägningen mellan enskildas rätt till skydd för sitt privat- och familjeliv och samhällets intresse av en effektiv brottsbekämpning är det betydelsefullt att med tillräckligt

> god precision kunna bedöma vilka resultat som användningen av hemliga tvångsmedel har lett till i berörda brottsutredningar. ”[48]

Skal man finne en presis balanse mellom behovet for å etterforske grov kriminalitet og borgernes rett til respekt for privatliv og korrespondanse, må det foreligge et presist datagrunnlag, så man kan fatte informerte beslutninger. Jeg vil i det følgende se litt nærmere på den tilgjengelige statistikken og andre datapunkter som omhandler bruken av trafikkdata i etterforskningsøyemed.

Når det gjelder statistikken er det flere likhetstrekk ved de erfaringer som er gjort i Sverige, Tyskland og Norge.[49] Studier fra alle disse landene indikerer at trafikkdata er nyttige i ca 40-50 prosent av tilfellene der de blir uthentet. Fra Danmark har jeg kun utleveringsstatistikken å lene meg på, jeg har ikke funnet kvalitative studier herfra.[50]

Det er noen grunnleggende problemer ved å vurdere både de kvalitative studiene og statistikken som foreligger. For det første sier tallene meg lite i relasjon til min problemstilling. Jeg må avgjøre om behovet for trafikkdata utgjør et presserende sosialt behov jf. EMK art 8, en undersøkelse der alternativene synes å ha vært "nyttig" og "ikke nyttig", vil gi lite veiledning i denne sammenhengen. Dette synes dog å være situasjonen i både Sverige, Tyskland og Norge, noe som indikerer et behov for ytterligere forskning på dette området. Et unntak fra dette er en uttalelse om KRIPOS:

> “KRIPOS har dokumentert at det ble innhentet trafikkdata i 52 prosent av 1.450 alvorlige straffesaker - der det ble ilagt straff for drap, narkotikaforbrytelse, ran eller seksuelle overgrep. I 82 prosent av disse sakene hadde trafikkdata stor betydning.” [51]

Denne uttalelsen går lengre i å spesifisere hva slags nytte og for hvilke typer forbrytelser nytten foreligger. Dette er mer relevant i relasjon til en EMK art. 8-drøftelse. De øvrige undersøkelsene jeg har sett på, gjelder alle typer lovbrudd og konkretiserer ikke nyttegraden. Tallene fra KRIPOS retter seg mot grov kriminalitet og har en mer spesifisert nytteterskel.

Det synes utvilsomt å være slik at trafikkdata kan anses for å være et mye brukt verktøy og et nyttig verktøy. I Danmark ble trafikkdata hentet ut i 1823 tilfeller i 2008.[52] At det danske politiet henter ut trafikkdata fem ganger daglig, indikerer at dette er et basisverktøy som blir

48 Regeringens skrivelse 2009/10:66

49 Rechtswirklichkeit der Auskunftserteilung uber Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO. NOU 2009:15. Regeringens skrivelse 2009/10:66.

50 Politiets årstabel 2009

51 http://www.dagsavisen.no/meninger/article489394.ece - jeg har kontaktet KRIPOS for å få tallmaterialet, men har ikke fått svar, dette er en mulig feilkilde.

52 Politiets årstabel 2008

jevnlig brukt. Tilsvarende ser det ut til å bli over 2000 tilfeller i Norge i 2010 om man ekstrapolerer fra første kvartal.[53]

Jeg vil i det videre se litt nærmere på statistikken fra Danmark (og EU forøvrig). Det første som slår meg når man ser gjennom statistikken fra Danmark når det gjelder uthenting av trafikkdata, er at den markante hovedvekten av datautlevering skjer på mobiltelefonifronten. Totalt ble det i 2008 utlevert data i 3489 tilfeller, og i 2009 ble det utlevert data i 4045 tilfeller. Av dette var det henholdsvis 91 prosent i 2008 og 93 prosent i 2009 mobildata. Ellers var fordelingen slik i 2008: 5,1 prosent for fasttelefoni, 3.5 prosent for ordinær Internettrafikk, 0,2 prosent for Internettbasert epost og 0.05 prosent for Internettelefoni. I 2009 var fordelingen slik: 3 prosent av datautlevering for fasttelefoni, 2,8 prosent for ordinær Internettrafikk, 0,2 prosent for Internettelefoni og 0.9 prosent for Internettepost. Dette er tall som også gjenspeiles av den foreløpige statistikken fra EU generelt.[54] Mobildata utgjør altså den store hovedvekten av de trafikkdata politiet bruker. Tilsvarende kan man se nærmere på når trafikkdata blir hentet ut. Den absolutte hovedvekt av data, i alle kategorier, blir utlevert fra 0-6 måneder, og om man bryter ned dette, er størsteparten av disse data utlevert fra 0-3 måneder. Dette indikerer, i likhet med de tallene fra den upubliserte rapporten fra EU, at trafikkdata blir hyppigst utlevert de første 3 måneder, dernest innenfor 6 måneder, og at søknader om utlevering skjer stadig mindre frekvent etter dette.

Hva brukes så trafikkdata til? I Danmark ble det i 2008 gjort totalt sett 4811 inngrep. Av disse var 37,89 prosent uthenting av trafikkdata (1823 tilfeller). Jeg vil se litt på hvilke kategorier av forbrytelser som er fremtredende og hvilke konsekvenser uthentingen har. Kategorien ”øvrige” er den mest fremtredende for alle overvåkingsinngrep. 47,43 prosent av inngrepene som blir gjort (Dette gjelder alle overvåkningsinngrep, men i mangel på mer detaljert statistikk forutsetter jeg at fordelingen er tilsvarende også for trafikkdata.) havner i kategorien ”øvrige”, der verken type eller alvorlighet blir definert. Den nest største gruppen er narkotikakriminalitet, der 37,02 prosent av alle tiltak havner. Her er det heller ingen videre inndeling av grovhet eller type narkotikakriminalitet. Det er et relativt stort hopp ned til de neste punktene på listen, drap med 7,98 prosent, grovt tyveri med 3,89 prosent, vold (en ganske bredt definert gruppe) med 2,47 prosent og sist kommer menneskesmugling o.l. og forvoldt fare med henholdsvis 0,96 prosent og 0,25 prosent.

Slik jeg tolker tallene er det vanskelig å komme med noen gode kvalitative konklusjoner rundt bruken av overvåkning generelt og trafikkdata spesifikt. Både gruppen ”øvrige” og ”vold” er så lite deskriptive at det er vanskelig å vurdere dem opp mot f.eks. ”serious crime” i direktivteksten. Begge deler spenner fra svært små og ubetydelige lovbrudd (besittelse av marihuana) til større og langt grovere forbrytelser (storstilt smugling og formidling av heroin). Jeg synes likevel at narkotikakriminalitet, drap og grovt tyveri, som utgjør nesten 50 prosent av uthentingen indikerer at det er en samfunnsnytte til stede. Det presise nivået er vanskelig å fiksere.

53 Høring om datalagringsdirektivet - Uttalelse fra Post- og teletilsynet

54 Room Document - Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communications.

I Norge kan man komme til en lignende konklusjon basert på en kombinasjon av tallmaterialet fra SSB og uttalelsene fra KRIPOS. Her fremgår det at trafikkdata hadde stor betydning i 82 prosent av tilfellene hvor det ble uthentet i relasjon til grov kriminalitet

Det er vanskelig å trekke klare konklusjoner ut av dette tallmaterialet. Et behov for mer forskning synes å være klart. Likevel vil jeg påstå at disse tallene og undersøkelsene viser at trafikkdata er et nyttig basisverktøy for politiet. Spesielt synes trafikkdata fra mobilkommunikasjon å være et sentralt etterforskningsverktøy. De øvrige kategorier er derimot mindre fremtredende i uthentingsstatistikken, både fra Danmark og Europa. Det er også verdt å merke seg at uthenting av data er nærmest fraværende etter seks måneder. Dette kan indikere at både alder og type trafikkdata er avgjørende for hvor viktig lagring er for politi- og påtalemyndigheter.

Som debatten i Norge har vist, er det lett å misforstå og feilrepresentere denne typen statistikk. Sammenligner man antall uthentinger med det totale antall lovbrudd i Norge eller Danmark, kan tallene synes å indikere at trafikkdata har marginal betydning i det store bildet. Det man må huske er at forenklede forelegg, der trafikkdata aldri vil bli etterspurt, dominerer statistikken. Tilsvarende kan man si om andre mindre alvorlige lovbrudd. Tar man høyde for slike faktorer, resulterer det i et mer presist bilde, som nok vil ligge tettere opp mot uttalelsene fra KRIPOS: trafikkdata har stor betydning for etterforskningen av grov kriminalitet.

4 Betydningen av EMK art. 8 ved implementeringen av datalagringsdirektivet.

4.1 Innledning

EMK art. 8 knesetter borgernes rett til respekt for privatliv, hjem, korrespondanse og familieliv.
Artikkelen er delt inn i to deler hvorav den siste delen også kan deles inn i to enkeltdeler. Det første leddet av artikkelen klargjør hva som beskyttes, nemlig privatliv, familieliv, hjem og korrespondanse. Det andre leddet hjemler inngrep såfremt de kumulative vilkår som fremgår blir tilfredsstilt. Tradisjonelt har EMD valgt å tolke første ledd utvidende og unntaksbestemmelsene i andre ledd strengt.1

I denne innledningen vil jeg søke å beskrive det rettslige grunnlaget for de innledende drøftelsene før proposjonalitetsvurderingen. Jeg vil ta utgangspunkt i ordlyden og rettspraksis fra EMD og kort belyse hva som ligger i art. 8.

Ordlyden i art. 8 er som følger:

> "**Art 8.** *Right to respect for private and family life*
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Tradisjonelt tar EMD utgangspunkt i ordlyden og følger det skjema den legger opp til. Jeg vil i denne innledningen søke å gjøre det samme. Jeg vil først se på hva beskyttelsesområdet omfatter og hva som utgjør inngrep. Videre vil jeg se på hvilke formål som anses for å være aktverdige. Jeg behandler både kravet til lovkvalitet og proporsjonalitet alene, så jeg vil kun overfladisk se på disse i denne innledningen.

Det første jeg vil se på, er beskyttelsesområdene og hva som utgjør inngrep. EMK art. 8 beskytter privatliv, familieliv, hjem og korrepondanse. Disse områdene har tradisjonelt blitt tolket utvidende av EMD. Art. 8 har blitt anført både når det gjelder adopsjonssaker, utvisningssaker, kommunikasjonsinngrep, inngrep i relasjon til seksualmoral og en hel rekke andre saker. Når det gjelder korrespondanse, er det også her et bredt spekter av forskjellige saker. Jeg vil først kort gå gjennom hva som legges i privatliv, familieliv og hjem, før jeg går litt nærmere inn på hva retten har definert som korrespondanse. Det er vanskelig å drøfte hva som beskyttes uten at man samtidig tar stilling til hva som utgjør inngrep, disse to faktorene vil dermed gli noe over i hverandre i vurderingene under.

Når det gjelder privatliv, har EMD en bred tolkning av hva dette innebærer. I Niemietz-dommen (CASE OF NIEMIETZ v. GERMANY *(Application no. 13710/88) §29*) fremgår det at ikke bare det man opplever i det helt private som omfattes, men også ens sosiale interaksjon i den omgangskrets man har. Dette innebærer også profesjonelle relasjoner og de relasjoner man har på arbeidsplassen. Harris (Harris, 2009, 366) har delt privatliv inn i seks kategorier: personlig identitet, moralsk eller fysisk integritet, personlig rom, innsamling og bruk av informasjon, seksualliv og sosiale relasjoner. Privatliv kan slik gli over i flere av de andre gruppene og grensene er her flytende. I flere dommer har også EMD valgt å ikke definere hvilket beskyttelsesområde det er snakk om, og nøyer seg med å anføre brudd på EMK art. 8 som grunnlag for den rettslige drøftelsen.

Beskyttelsen av familieliv, har gjennomgått en utvikling i takt med de sosiale, kulturelle og religiøse endringer i det europeiske storsamfunnet de siste tiår. I X, Y and Z-saken (X, Y and Z v. the United Kingdom, 21830/93, §36) fremgår det at det ikke bare er de tradisjonelle biologiske familier som nyter godt av beskyttelse, men også nye konstellasjoner der det de facto er familiære bånd. Det fremgår av rettspraksis at reasjoner til fjernere slektninger også nyter godt av beskyttelsen, men at inngrepstersklen blir lavere jo fjernere bånd individene har

seg imellom. Det er dog ingen skjematisk løsning her. Det er de de facto forhold som legges til grunn, ikke slektskap på papiret.

Borgerne nyter også godt av beskyttelse av sitt hjem. Av Giacomelli-dommen (CASE OF GIACOMELLI v. ITALY *(Application no. 59909/00), §76)* fremgår det at et "hjem" er et fysisk avgrenset sted hvor man kan utvikle og vedlikeholde privatliv og familieliv. Individer har rett til respekt for dette hjemmet. Denne beskyttelsen innebærer ikke bare beskyttelse mot ulovlig inntrengning og andre fysiske inngrep, men også en beskyttelse mot støy, lukt, forurensning o.l. Her avgjør grensen for hva som utgjør et inngrep om man befinner seg i kjernen av beskyttelsen eller i randsonen, hvilke konsekvenser handlingen har. I likhet med de fleste andre vurderinger bærer denne i rettspraksis av å være av en veldig konkret art. EMD ser på hva som de facto har skjedd og veier forskjellige momenter opp mot hverandre.

Korrespondanse beskyttes også av art. 8. Hva som ligger i begrepet korrespondanse har blitt utvidet gjennom rettspraksis til noe mer enn bare innhold i brev/telefonsamtaler. Av Malone-saken fremgår det at bl.a. metering-informasjon beskyttes av EMK art. 8.[55] Dette inkluderer hvilke nummer man har ringt til, når man har ringt og annen informasjon utover innholdet i kommunikasjonen. Dette inntrykket forsterkes av Copland-dommen, der lagring av dato for oppringninger og samtalelengde ble ansett for å være tilstrekkelig til å fastslå at et inngrep forelå.[56] EMD bruker sådan en forholdsvis lav terskel for hva som kan anses for å være "korrespondanse" og i tillegg for hva som utgjør et inngrep. Det fremgår også av Copland-dommen at det ikke er nødvendig at overvåkningsdata blir brukt for at det inngrep skal foreligge, lagring utgjør alene et inngrep. Det synes dermed å være klart EMD, i tråd med de generelle prinsipper om utvidende tolkning, har lagt et bredt korrespondanse-begrep til grunn.

Når det gjelder kravet til formål, er opplistingen av aktverdige formål så bred at det sjelden er her striden står. Det er få tiltak som ikke kan sies å være av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter. Jeg kan ikke si å ha sett noen dommer som har diskvalifisert et inngrep som følge av at formålet ikke var aktverdig. Det indikerer at terskelen for å godta de formål som anføres fra statenes side er forholdsvis lav og at dette sjelden kommer på spissen.

4.2 Beskyttelsesområdet

Jeg vil i dette og de to neste avsnitt forsøke å holde direktivet opp mot den tolkning av EMK art. 8 jeg har redegjort for over.

Det fremgår av første ledd at alle skal ha rett til respekt for privatliv, familieliv, hjem og korrespondanse. Det er da særskilt "korrespondanse" som er relevant for min oppgave.

Det fremgår av konvensjonsteksten at det skal foreligge en rett til respekt for korrespondanse. En av de sentrale dommene for min problemstilling er Malone-dommen, dette er en dom som

55 CASE OF MALONE v. THE UNITED KINGDOM *(Application no. 8691/79) §84*
56 Copland v. the United Kingdom, 62617/00, §43

omhandler uthenting av "data obtained by metering".[57] Dette er i motsetning til ordinære innholdsdata fra telefonovervåkning, trafikkdata fra en ordinær telefonsamtale. Det som blir registrert er hvem det ringes til (eventuelt hvem som ringer til den avlyttede), når samtalene finner sted og hvor lenge de varer. Datalagringsdirektivet påbyr lagring av denne typen data, samt lokasjonsdata i tillegg til en del andre data. Man kan dermed si at lagringsplikten etter direktivet i stor grad overlapper med "data obtained by metering" slik det fremgår i denne dommen. EMD sier dette om lagring av slike trafikkdata:

> "The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8 (art. 8). The records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the concent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (art. 8)."

Slik jeg tolker dommen, anser EMD trafikkdata for å være en sentral del av telefonkommunikasjon og sådan en del av korrespondansen som beskyttes etter første ledd. (Videre legger også domstolen til grunn at utlevering av denne typen informasjon er et inngrep i relasjon til art. 8, andre ledd, men dette vil jeg komme tilbake til under). Sådan vil overvåkning, lagring og/eller uthenting av lignende data konstituere et inngrep i rettighetene etter første ledd. Trafikkdataene som blir omtalt for analoge telefontjenester i denne dommen, er i direktivet også objekt for lagringsplikten, i tillegg har man sterke paralleller til "data obtained by metering" i IP-adresser, påloggingstidspunkt og andre data som ellers lagres under datalagringsdirektivet. Det fremgår som forholdsvis klart, slik jeg tolker direktivet i lys av denne dommen og annen rettspraksis, at disse data vil falle inn under EMK art. 8s beskyttelse.

4.3 Inngrep

Det er en forutsetning for at en handling (eller ikke-handling) skal bryte med EMK art. 8 at den konstituerer et inngrep. Jeg vil her søke å drøfte om lagring og uthenting av trafikkdata konstituerer et inngrep. Jeg vil først se på om påbud om lagring av trafikkdata alene kan utgjøre et inngrep. Slik jeg tolker Copland-dommen, synes det å foreligge liten tvil om dette.[58] Her fremgår det at lagring av informasjon om når og til hvem noen har ringt, i seg selv er et inngrep. Dette uavhengig av om denne informasjonen blir brukt senere. Dette fremgår også bl.a. av Amann-dommen der lagring av kommunikasjon ble ansett for å være et inngrep, uavhengig av videre bruk.[59]

Når det gjelder utlevering av trafikkdata, synes dette også å være forholdsvis klart innenfor inngreps-definisjonen. Dette fremgår bl.a. av Malone-dommen:

57 Malone v. The United Kingdom Application No: 8691/79
58 Copland v. the United Kingdom, 62617/00, §43
59 Case of Amann v. Switzerland (Application no. 27798/95)

> "Consequently, release of that information to the police without the concent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (art. 8)."

Det er to ting jeg vil henlede oppmerksomheten mot i dette sitatet. Det første, og kanskje viktigste, er at utlevering av trafikkdata til politiet anses for å være et inngrep. Det andre poenget man kan dedusere fra sitatet, er at det ikke nødvendigvis er politiet som må foreta lagringen. Rutinemessig lagring fra kommunikasjonstilbydere, såfremt lovverket som åpner for utlevering til myndighetene, er tilstrekkelig for å legge til grunn at et inngrep har funnet sted.

Videre kan man merke seg at det ikke er nødvendig med konkrete handlinger for at et inngrep skal foreligge:[60]

> "Furthermore, in the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menance of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for private and family life and for correspondence."

Det er naturlig å tolke denne dommen fra EMD dit hen at det ikke er nødvendig med aktuelle og konkrete inngrep hjemlet i direktivet. Et implementeringslovverk som legger grunnlaget for tvungen lagring og potensiell uthenting utgjør isolert sett et inngrep. Dette innebærer at selve trusselen om lagring av trafikkdata er tilstrekkelig for å definere dette som et inngrep.

Det er dermed, slik jeg tolker både Klass-dommen og Copland-dommen lite som tilsier at man ikke skal anse tvungen lagring av trafikkdata som et inngrep etter EMK art. 8. Myndighetene pålegger kommunikasjonstilbyderne å lagre data. I tillegg åpnes det får en praksis der politi- og påtalemyndigheter kan hente ut disse data.

4.4 Formålskravet

Hvis en stat skal foreta unntak fra første ledd i art. 8 og gjøre inngrep i rettighetene i første ledd, er det en forutsetning at det blir gjort i henhold til de aktverdige mål som blir listet opp i andre ledd:

60 Klaas v. Germany Application No: 15473/89

> "[..]av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter."

Generelt kan man si at det tradisjonelt har vært få uenigheter på dette området i rettspraksis fra EMD. De fleste tiltak som blir iverksatt av statene kan defineres som å møte ett eller flere av disse kravene. EMD bruker sjelden mye tid på å diskutere hvorvidt målsetningene er reelle eller aktverdige. Om statene anfører at de søker å øke nasjonal sikkerhet, offentlig trygghet etc., er det sjelden domstolen overprøver dette ytterligere.[61]

Når det gjelder datalagringsdirektivet kan man anføre hensyn til den nasjonale sikkerhet, landets økonomiske velferd (harmonisering av utgifter til pålagt lagring for ekomtilbydere) og målet om å forebygge uorden eller kriminalitet. Det er liten tvil om at disse målsetningene må anses for å være i tråd med kravene i EMK art. 8, andre ledd.

4.5 Lovkrav

4.5.1 Innledning

Det fremgår av unntaksreglene i EMK art. 8, andre ledd, at et av kravene er at inngrep må hjemles i lov. Dette kravet har gjennom rettspraksis blitt utviklet til å inneholde flere distinkte krav. Det er her snakk om tilgjengelighet, presisjon som leder til forutberegnelighet for borgerne og et kvalitetskrav som skal beskytte borgerne mot vilkårlige inngrep. Jeg skal videre i dette kapittelet utdype hva som ligger i disse begrepene og se nærmere på hvorvidt forskjellige innføringsløsninger kan sies å tilfredsstille disse kravene. Den røde tråden også her, er å se hvorvidt det er mulig å harmonisere datalagringsdirektivet med EMK art. 8. Det er lite som tilsier at det er problematisk å forfatte lovverk om lagring av trafikkdata om man gjør et grundig forarbeide. Likevel vil jeg trekke frem endel problemområder som har dukket opp hos flere medlemsland når det gjelder lovkvalitet.

Et stort problem når det gjelder lovgivning på dette område er hvorvidt man praktisk kan konstruere lover på et så teknologisk dynamisk område, som er presise nok uten at de må oppdateres veldig jevnlig for å ha den funksjonen de er tilsiktet. Spesielt når det gjelder kommunikasjonsteknologi er denne faren påtagelig. Man kan her bruke Internett som et godt eksempel. Vil vi ha en lignende struktur, både rent fysisk, men også når det gjelder programvaren som styrer vår kommunikasjon, om fem, ti eller femten år? Mer og mer av det vi gjør på Internett foregår i den såkalte "skyen", der lokale leverandører ikke har tilgang til eller oversikt over hva som skjer. Man kan nok besvare dette spørsmålet med et relativt ubetinget: nei. Er kravet til spesifikk lovgivning så strengt at det i praksis blir nærmest umulig å implementere direktivet på en fungerende måte? Det blir her vanskelig å finne balansen

61 Se f.eks. Klaas v. Germany Application No: 15473/89

mellom kravet til forutberegnelighet og klarhet og en rent praktisk mulighet for å kunne forfatte regler som fungerer over en lengre tidshorisont.

4.5.2 Tilgjengelighet og presisjon

For det første, som det fremgår av ordlyden i konvensjonen, er det et krav til at det må foreligge en lov som hjemler inngrepet. Dette er forutsetningen for de to andre kravene, som ble klart definert i Sunday Times-dommen :

> "First, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail"[62]

Her fastslår EMD at det ikke er tilstrekkelig at det foreligger en lov som regulerer inngrepet. Loven må i tillegg både være presis nok til at borgene skal kunne forutse sin rettsposisjon, om så med kompetent rådgivning. Forutsigbarhet og forutberegnelighet blir sådan sentrale momenter når man skal vurdere kvaliteten på lovgivning. Kravet til lovkvalitet har senere i rettspraksis blitt ytterligere utvidet, og inkluderer krav til at lovverket inkluderer skranker som skal sikre borgerne mot vilkårlige inngrep.[63] Det stilles i flere saker konkrete krav til regulering av fremgangsmåte ved inngrep i rettigheter etter konvensjonen. Jeg skal gå nærmere inn på hvorvidt de forskjellige implementeringsløsninger kan anses å møte disse kravene under.

Et annet moment som kan være verdt å nevne når det gjelder alle de kravene EMD stiller til nasjonale lovverk, er deres relative natur. Dette fremgår bl.a. av Gubi-dommen.[64] Kravet til presisjon og øvrige krav til lovkvalitet, avhenger av inngrepet som gjøres og interessen det gripes inn i. Er det et inngrep som rammer bredt (eller altomfattende) og griper inn i sentrale rettigheter, stilles det dermed strengere krav til presisjon og øvrige kvalitetskrav som skal hindre vilkårlige inngrep. Når det gjelder datalagringsdirektivet, omfatter det alle borgerne i medlemsstatene og griper inn i deler av en konvensjonsbeskyttet rettighet som i flere dommer blir ansett som en kjernerettighet.[65] Jeg vil derfor legge til grunn at kravene til lovverket som regulerer inngrepet vil være strenge.

---

62 CASE OF THE SUNDAY TIMES v. THE UNITED KINGDOM (Application no. 6538/74)

63 Se bl.a. Iordachi and others v. Moldova. (25198/02), CASE OF KRUSLIN v. FRANCE (Application no. 11801/85) og CASE OF KLASS AND OTHERS v. GERMANY (Application no. 5029/71)

64 CASE OF VEREINIGUNG DEMOKRATISCHER SOLDATEN OSTERREICHS AND GUBI v. AUSTRIA Application no. 15153/89))

65 Se f.eks. Monoroy-dommen, Handyside-dommen m.v.

Alle medlemsstatene jeg har undersøkt har innført direktivet i lovs form og har sådan tilfredsstilt det mest grunnleggende lovkravet. Jeg har ikke hatt problemer med å finne de forskjellige lovverk, og kan sådan ikke utsette noe på tilgjengeligheten. De to grunnleggende kravene som er utgangspunktet for drøftelsen, er derfor tilfredsstilt hos de statene jeg har undersøkt. Det er derfor lite som taler for at en harmonisering av de forpliktelsene Norge har i forhold til EMK og de forpliktelsene man eventuelt vil ta på seg i relasjon til direktivet vil komme i motstrid her.

Det neste momentet blir sådan å vurdere om lovene kan være presise nok til at borgerne kan forutse sin rettsposisjon. Lovverket må være tilstrekkelig presist til at borgerne vet hvilke handlinger som kan føre til at deres trafikkdata hentes ut og vite hvilke data som står i fare for å hentes ut. Her er det forskjellig praksis blant EU-landene. [66] Det er store variasjoner når det gjelder hvilke lovbrudd som kan føre til uthenting av trafikkdata. Fra ett års strafferamme[67] til femårs strafferamme.[68] Det er i tillegg noen av medlemslandene som har valgt å ikke definere noen strafferammegrense eller øvrige former for terskler, men lar domstolene selv definere hva "serious crime" utgjør.[69] Varierende strafferammeterskler i medlemslandene er i seg selv ikke problematisk. Derimot har det formodningen mot seg at å basere seg på rettspraksis er tilstrekkelig. Som nevnt tidligere vil EMD sette spesielt strenge krav til lovgivning som regulerer inngrep på sensitive områder og inngrep som omfatter store deler av befolkningen, datalagringsdirektivet møter begge disse kriterier. Dette fremgår bl.a. av Kruslin-dommen:

> "Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated." [70]

Her fremgår det at klare, detaljerte regler er essensielt når det gjelder overvåkning av telefonkommunikasjon, dette vil også kunne appliseres på andre kommunikasjonsformer etter mitt syn. Domstolen henviser spesifikt til "other forms of interception" og viser samtidig til den teknologiske utviklingen. Det er derfor naturlig å tillegge denne uttalelsen vekt i relasjon til ordinær Internettrafikk, bredbåndstelefoni og lignende former for kommunikasjon som er eksempler på ny teknologi.

Slik jeg tolker rettspraksis, vil dette medføre at implementeringsløsninger der terskelen er helt og holdent gitt domstolenes praksis, mest sannsynlig ikke vil anses for å møte EMKs krav til lovkvalitet. Selv om man tidlig får rettspraksis om enkeltsaker, er det tvilsomt om dette vil skape forutberegnelighet. Det har formodningen for seg at rettspraksis på dette området vil

66 Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communication.
67 F.eks Frankrike og Nederland
68 F.eks Belgia og Kypros
69 F.eks Tsjekkia, Estland og Malta
70 CASE OF KRUSLIN v. FRANCE (Application no. 11801/85)

være av spesifikk og konkret art. Det vil dermed være vanskelig å ekstrapolere allmenngyldige regler fra denne praksisen. En tilsvarende problemstilling oppstår der man har generelle supplerende bestemmelser til de ordinære strafferammetersklene. Romania valgte en innføringsmodell der "også andre forbrytelser som truer rikets sikkerhet" var en del av grunnlaget, dette ble ikke godtatt av den nasjonale forfatningsdomstolen, som nevnt tidligere. Denne typen innføringsmodeller gir myndighetene et nærmest ubegrenset rom for skjønn og skaper en lite forutberegnelig situasjon for borgerne. Dette synet underbygges av uttalelser i Iordachi-dommen. Slik jeg ser det er det vanskelig å harmonisere denne typen bestemmelser med EMK art. 8. I tillegg til Iordachi-dommen[71], finner jeg også holdepunkter for dette synet i Kruslin-dommen.[72] Det å lovfeste domstolsbehandling eller en lignende uavhengig og kontradiktorisk prosess synes dermed å være en forutsetning for å unngå motstrid mellom direktivet og EMK art. 8.

Det neste momentet når det gjelder presisjon, er spørsmålet om hvilke data som lagres og dermed kan hentes ut. Nederland og Slovakia rapporterer bl.a. begge om uvisshet rundt hvilke data som skal lagres, dette indikerer at det er rom for flertydighet i direktivet når det gjelder hva som skal lagres og at denne usikkerheten forplanter seg ned i de nasjonale systemer.[73] Jeg har ikke tilstrekkelig data fra verken Nederland eller Slovakia til å konkludere om disse landenes presisjonsnivå når det gjelder hva som lagres, men at de selv rapporterer usikkerhet er en indikasjon på problemet. De øvrige medlemsland jeg har sett nærmere på, har regulert hva som skal lagres forholdsvis utstrakt og i stor detalj. Det er dermed forholdsvis enkelt for borgerne å forutse hvilke data som kommer til å lagres.

Avslutningsvis vil jeg kort nevne at EMD i Iordachi-dommen understreker viktigheten av regler som regulerer graden av mistanke som er nødvendig for å hjemle overvåkning.[74] Her kritiseres moldovsk lov for å mangle retningslinjer for hvor stor grad av mistanke som er nødvendig for å tillate avlytting. Av de landene jeg har undersøkt, er det kun Danmark som synes å ha spesifikke regler for dette i forbindelse med direktivinnføringen. De øvrige land regulerer dette i den generelle prosesslovgivning. Det har formodningen for seg at de generelle straffeprosessuelle regler vil være tilstrekkelige. Det kan dog være naturlig å anbefale endringer eller tillegg i straffeprosesslovgivning for å sikre at utlevering kun skjer ved kvalifisert mistanke. Det norske lovforslaget som nylig kom på banen, ser ikke ut til å kreve dette i alle tilfeller. Sågar gis PST mulighet til uthenting til forebyggende formål.

4.5.3 Kvalitetskrav

EMD har gått videre fra presisjonskravet til også å innfortolke et kvalitetskrav i art. 8. Kvalitetskravet innebærer at statene forplikter seg til å forfatte lover som inneholder

71 Iordachi and others v. Moldova. (25198/02) §51
72 KRUSLIN v. FRANCE(Application no. 11801/85) §36).
73 Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communication.
74 Iordachi and others v. Moldova. (25198/02) §51

tilstrekkelige sikkerhetsmekanismer som skal sikre borgerne mot vilkårlige inngrep.[75] Det er i hovedsak to poeng som er sentrale her. For det første at det må foreligge uavhengig kontroll, fortrinnsvis domstolskontroll, med inngrep som foretas. Videre at lovene som regulerer inngrepet i tilstrekkelig grad hindrer misbruk av lagrede trafikkdata.

Når det gjelder kommunikasjon med journalisters hemmelige kilder og lignende situasjoner, har jeg tidligere vært inne på dette. Dette er et område som er lovteknisk vanskelig å regulere. For det første må man vurdere om det er mulig å sikre advokater, journalister og lignende grupper mot lagring. I fall dette ikke er mulig, må man undersøke hvordan man skal sikre at data av denne typen ikke blir utlevert. For det andre er lagring av denne typen trafikkdata (f.eks. kommunikasjon med vernede kilder) et vurderingstema under proporsjonalitetsdrøftelsen. Hvis man ikke kan sikre at denne typen trafikkdata kan unntas fra lagring, er det en faktor som veier i negativ retning i forbindelse med proporsjonalitetsdrøftelsen. Senere i dette kapittelet vil jeg gå nærmere inn på mulighetene for å unnta denne typen kommunikasjon.

Jeg vil først gå nærmere inn på hva EMD sier om domstolsbehandling og uavhengig kontroll av inngrep. Det fremgår av flere dommer på overvåkningsområdet, at EMD legger stor vekt på at lovverket garanterer uavhengig kontroll med overvåkningstiltak. Dette fremgår kanskje klarest i Klass-dommen:

> "The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge."[76]

EMD tilkjennegir en preferanse for domstolskontroll med denne typen inngrep. Et uavhengig organ blir godtatt, men i prosessen fremheves ønsket om at en domstol bør ivareta denne kontrollfunksjonen. Også i saker som gjelder nasjonal sikkerhet, er dette et prinsipp som tillegges vekt, dette fremgår av bl.a. denne uttalelsen fra Al-Nashif-dommen:

> "Even where national security is at stake, the concepts of lawfulness and the rule of law in a democratic society require that measures affecting fundamental human rights must be subject to some form of adversarial proceedings before an independent body competent to review the reasons for the decision and relevant evidence, if need be with appropriate procedural limitations on the use of classified information"[77]

75 Se bl.a. Iordachi and others v. Moldova. (25198/02), CASE OF KRUSLIN v. FRANCE (Application no. 11801/85) oEMK art. 8 knesetter borgernes rett til respekt for privatliv, hjem, korrespondanse og familieliv. Artikkelen er delt inn i to deler hvorav den siste delen også kan deles inn i to enkeltdeler. Det første leddet av artikkelen klargjør hva som beskyttes, nemlig privatliv, familieliv, hjem og korrespondanse. Det andre leddet hjemler inngrep såfremt de kumulative vilkår som fremgår blir tilfredsstilt. Tradisjonelt har EMD valgt å

76 CASE OF KLASS AND OTHERS v. GERMANY (Application no. 5029/71)

77 CASE OF AL-NASHIF v. BULGARIA (Application no. 50963/99)

Slik jeg tolker denne dommen, understreke viktigheten av en kontradiktorisk rettsprosess når det gjelder inngrep i fundamentale menneskeretter, selv om dette innebærer en prosess for lukkede dører for å sikre konfidensialitet.

Mitt syn etter dette, er at lovverk som implementerer datalagringsdirektivet som et minstekrav må inneholde regler som påbyr domstolsbehandling (eller behandling i lignende, uavhengige organer) av utleveringskrav for å kunne harmoniseres med de krav EMK art. 8 stiller. Jeg ser ikke bort fra at unntaksbestemmelser i hastesaker o.l. vil være fullt ut akseptabelt, men det er nærliggende å anta at løsninger som den finske, der man ikke har noen form for domstolskontroll av data, ikke er tilstrekkelig for å møte EMKs krav til lovkvalitet. Dette vil også være et vurderingstema under proporsjonalitetsdrøftelsen.

Det neste vurderingstemaet når det gjelder lovkvalitet, er kravene til ytterligere regulering av lagring og uthenting av trafikkdata. EMD har i den rettspraksis som foreligger i relasjon til overvåkning satt flere krav til de nasjonale lover som regulerer overvåkningspraksis, utlevering av data, bruk av data internt hos politiet og sletting av data etter endt bruk. Den første problemstillingen i så måte, er å drøfte om det er mulig å sikre advokatprivilegiet og pressens kildevern. Er det teknisk mulig å unnta disses kommunikasjonsdata fra lagring? Slik jeg ser det, er dette i beste fall svært vanskelig. Denne typen kommunikasjon kan skje fra hjemmetelefon, personlige mobiltelefoner eller på annet vis. Mulighetene for problemer i forhold til unntaksregler er dermed mange. Det som gjenstår er dermed siling av denne typen data, slik at de kun lagres, og ikke kan være gjenstand for uthenting. Dette er en problemstilling som ligger tett opp mot en uttalelse fra Iordachi-dommen. Iordachi-dommen er en sentral dom, og jeg vil derfor greie raskt ut om bakgrunnen for denne dommen i EMD.[78] Iordachi and others var en gruppe menneskerettsadvokater som jobbet for å avdekke menneskerettsbrudd i Moldova, de anså det som sannsynlig at deres kontorer ble avlyttet. Som en følge av overvåkningstrusselen (det nasjonale lovverk åpnet for slik overvåkning), gikk disse advokatene til sak. Dommen er relevant for min oppgave på mange punkter, men jeg vil spesielt peke på dette sitatet:

> "The Court is struck by the absence of clear rules defining what should happen when, for example, a phone call made by a client to his lawyer is intercepted."

EMD angriper her mangelen på prosedyrer og regelverk som regulerer hva som skjer når man fanger opp trafikkdata etter kommunikasjon mellom en klient og en advokat. Går man fra denne spesifikke anvendelsen og til et mer generelt prinsipp, kan det være naturlig å anta at forholdet til sensitiv kommunikasjon som lagres, bør lovreguleres. Dette medfører at en innføring av direktivet, for å være i tråd med EMK art. 8, bør lovregulere dette forholdet.

Jeg vil raskt drøfte forholdet til mer spesifikke regelverk for lagringssikkerhet. Dette gjelder både hos leverandører før uthenting og hos politi- og påtalemyndigheter etter uthenting. Også

78 Iordachi and others v. Moldova. (25198/02)

her er Iordachi-dommen relevant.[79] Her kritiserer EMD bl.a. mangel på tiltak for å sikre integriteten til overvåkningsdata og manglende regler om når data skal destrueres. Det synes å være et gjennomgående tema i dommer som omhandler overvåkning at regulering av hvordan data behandles/sikres hos leverandør, hos politi- og påtalemyndigheter og når/hvordan data skal destrueres, er viktig. [80] Uttalelser i andre dommer synes å forsterke dette inntrykket.[81] Slik jeg ser det, bør man ta høyde for dette ved en innføring av direktivet. Regulering som sikrer at trafikkdata ikke kommer på avveie fra kommunikasjonsleverandørene. Regler som sikrer forsvarlig bruk og lagring innad i politiet og regler som sikrer at trafikkdata blir slettet så snart politiet er ferdig med dem.

4.6 Konklusjon

Det er flere problemstillinger som må løses når det gjelder lovkvalitet. Tilgjengelighet og forutberegnelighet er forholdsvis uproblematisk. Det å regulere sikkerhetsmekanismer på en egnet måte, kan vise seg å være vanskeligere. Spesielt kan det å sikre seg mot lagring av trafikkdata fra advokat-klient-kommnikasjon, presse-kilde-kommunikasjon og lignende tilfeller bli vanskelig. Jeg kan ikke se for meg noen tekniske løsninger som vil fungere tilfredsstillende her. Man kan søke å begrense lagringen av slike trafikkdata ved å ha lister man kan søke om å være på, men dette vil nok kun løse deler av problemet. En bedre løsning kan være å filtrere ut denne typen kommunikasjon i domstolskontrollen. Lagring vil da likefullt foregå, med de problemstillinger det reiser. Sensitive trafikkdata kan sådan være tilgjengelige for ulovlig tilgang, misbruk og lekkasjer.

Et annet problem som er gjennomgående i de land jeg har sett nærmere på, er manglende regulering i forhold til å sikre trafikkdatas integritet fra de lagres hos leverandør til de brukes hos politi- og påtalemyndighet. Slik jeg tolker EMD bør lovpålagte tekniske løsninger som sikrer at data ikke blir manipulert være en del av innføringen av datalagringsdirektivet. Sabotasje eller manipulering av bevis vil være en reell risiko, løsninger med filsignaturer eller lignende teknologi kan på lang vei sikre at data ikke blir manipulert. Her er det mange utfordringer og her bør det nok jobbes aktivt med det IT-faglige miljøet for å få løsninger som ivaretar de behov som foreligger.

I relasjon til de andre kumulative krav, er det liten grunn til å utdype ytterligere. Det hersker liten tvil om at påbudet om lagring er et inngrep, at trafikkdata nyter godt av beskyttelse som korrespondanse og at formålene med direktivet er aktverdige.

79 Iordachi and others v. Moldova. (25198/02).
80 Se bl.a. Kruslin-dommen, Iordachi-dommen, Klass-dommen m.v.
81 Se f.eks. CASE OF KOPP v. SWITZERLAND (13/1997/797/1000) og CASE OF HUVIG v. FRANCE (Application no. 11105/84)

5 Proporsjonalitetsvurderingen

5.1 Innledning

Jeg har valgt å dele proporsjonalitetskapittelet inn i to deler. I den første delen vil jeg prøve å gå gjennom de faktorene som avgjør hva slags skjønnsmargin statene gis ved en prøving av nødvendighets- og proporsjonalitetskriteriene for EMD. Jeg vil her gå gjennom noen faktorer fra rettspraksis som EMD tradisjonelt har brukt for å klargjøre skjønnsmarginen. I den andre delen vil jeg konkret vurdere nødvendighet og proporsjonalitet. Jeg vil først se nærmere på hvordan EMD tradisjonelt foretar denne drøftelsen, for så å trekke inn momenter fra de foregående kapitler i subsumeringen. Det er i dette kapittelet den viktigste drøftelsen vil ligge, da de øvrige kumulative vilkår i mindre grad er et stridstema. Jeg vil ta en del forbehold i løpet av spesielt andre del av dette kapittelet, da dette i stor grad er upløyd mark, og jeg må støtte meg på rettspraksis som er parallell eller analog, men som dog ikke nødvendigvis gir mulighet for noen fasitsvar. Målsetningen med dette kapittelet å gå gjennom de mest sentrale og relevante vurderingstemaene, peke på argumenter for og mot. Jeg vil i stor grad la de klare slutningene være underordnet.

5.2 Skjønnsmargin

5.2.1 Innledning

Det har siden 70-tallet utviklet seg en doktrine når det gjelder skjønnsmarginen for proporsjonalitetsvurderinger i EMD. Denne doktrinens innhold og historikk blir belyst bl.a.av Michael R. Hutchinson.[82] Den første saken hvor denne doktrinen tok form, var Handyside-dommen.[83] EMD gir statene en skjønnsmargin når det gjelder inngrep i rettighetene etter konvensjonens unntaksregler. Hvor stort dette skjønnsrommet, eller alternativt hvor strengt EMD rettslig prøver inngrep, avhenger av en rekke faktorer. Retten har tradisjonelt bl.a. lagt vekt på rettigheten det gripes inn i, formålet for inngrepet og hvor objektivt målbar inngrepets målsetning er. Det at statene tillates en skjønnsmargin, er en naturlig følge av at det ligger statene nærmest å vurdere hva som er nødvendige og proporsjonale tiltak til enhver tid. Det er statene som ligger nærmest i å balansere de forskjellige konkurrerende rettigheter og interesser på en god måte. En forutsetning for at dette kan gjøres effektivt er at statene gis et handlingsrom. En viktig del av drøftelser knyttet opp mot potensielle krenkelser av EMK blir dermed å avgjøre hvor strengt statenes inngrep skal prøves.

I denne delen av oppgaven vil jeg altså prøve å komme frem til hvor streng rettslig prøving det er sannsynlig at EMD vil gi en eventuell innføring av direktivet. Jeg vil gå nærmere inn på de relevante faktorer, og avslutte med å forsøksvis veie dem opp mot hverandre. Når det gjelder datalagringsdirektivet, er det flere faktorer som spiller inn på begge sider. Dette gjør at jeg ikke nødvendigvis kan gi noen klare svar.

De faktorene jeg vil se nærmere på er interessen inngrepet søker å beskytte, inngrepets natur, rettigheten det gripes inn i og hvorvidt interessen som beskyttes av inngrepet er objektivt

82 Hutchinson, 2008, The Margin of Appreciation Doctrine in the European Court of Human Rights
83 CASE OF HANDYSIDE v. THE UNITED KINGDOM (Application no. 5493/72) §48

målbar. Det er andre faktorer som blir lagt vekt på i rettspraksis, men for min problemstilling synes disse å være de mest relevante. Det kan synes at dette er lignende vurderinger og valg av faktorer som Kjølbro[84] og Harris[85] legger til grunn for skjønnsromsvurderingen.

5.2.2 Interessen inngrepet søker å beskytte

Det fremgår bl.a. av Gillow-dommen at interessen inngrepet søker å beskytte er relevant for hvor stor skjønnsmargin statene vil få ved en rettslig prøving.[86] Direktivets formål er formulert slik:

> "This Directive aims to harmonize Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law."

Målet er å bekjempe grov kriminalitet. Man søker å ivareta myndighetenes mulighet til å forutse, forhindre og etterforske grov kriminalitet både internt og på tvers av landegrensene. En sentral vurdering i forhold til interessen man søker å beskytte, er hvorvidt denne er en konvensjonsbeskyttet rettighet (og i så fall, en eksplisitt eller implisitt beskyttet rettighet) eller en rettighet som ikke er konvensjonsbeskyttet. Chassagnou-dommen fastslår at skjønnsrommet bl.a. avhenger av hvilke interesser inngrepet søker å beskytte.[87]

Slik jeg tolker dommen, sier EMD her at i de tilfeller der to konvensjonsbeskyttede rettigheter står mot hverandre, så må statene ha en bred skjønnsmargin for og best mulig kunne avveie de aktuelle interesser mot hverandre i lys av de nasjonale forhold som gjør seg gjeldende. Statene står i en særstilling da de er nærmere faktum og i større grad kan gjøre gode avveininger. De situasjoner der en konvensjonsbeskyttet rettighet står mot en rettighet som ikke eksplisitt er nevnt i konvensjonen, er derimot situasjonen en annen. Her skal det svært mye til ("only indisputable imperatives") før man kan godta inngrep. Jeg finner støtte for dette i Chassagnou-dommen. Det er spesielt ordet "enunciated" jeg anser for å indikere dette. Valget av dette ordet kan tyde på at domstolen setter implisitte rettigheter på en lavere trinnhøyde enn de eksplisitt og klart definerte rettigheter i konvensjonen. Tilsvarende bruker EMD også uttrykket "expressly guarantee" senere i den sammen dommen, som en beskrivelse av rettigheten som er garantert av konvensjonen som en motsetning til interessen den franske staten søkte å beskytte. Det er dog verdt å nevne at saken her omhandler et tiltak fra myndighetenes side som søkte å øke demokratisk deltagelse i jakt. Det er et stort spenn fra denne interessen til direktivets målsetning om å bekjempe grov kriminalitet. Man kan argumentere for at demokratisk tilgang og adgang til jaktområder er en form for organisasjonsfrihet, men jeg vil ikke gå nærmere inn på det her.

84 Kjølbro, 2007, s 522
85 Harris, 2009, s 349
86 CASE OF GILLOWv. THE UNITED KINGDOM*(Application no. 9063/80)*
87 Chassagnou and others v. France 1999. §113

Jeg vil i det videre først se nærmere på hvorvidt man kan anse beskyttelse mot grov kriminalitet for å være en konvensjonsbeskyttet rettighet. EMD har i flere saker innfortolket en plikt til å forebygge og etterforske grov kriminalitet i art. 2. Det er naturlig å tolke dette dit hen at beskyttelse mot grov kriminalitet som truer borgernes liv og helse, er en implisitt del av art. 2. Osman-dommen er her et godt eksempel.[88] Denne dommen klargjør at det ikke bare foreligger en negativ plikt for statene til ikke å delta i forsettelige og ulovlige drap, men at det også foreligger en plikt til å ta de nødvendige steg for å sikre livene til sine borgere. Samtidig tar domstolen det forbehold at forholdet til bl.a. art. 8 må ivaretas i denne prosessen.

Det er verdt å merke seg at uavhengig av hvorvidt retten til å bli beskyttet fra grov kriminalitet er konvensjonsbeskyttet eller ei, så har det kommet flere dommer som poengterer at nasjonal sikkerhet og bekjempelse av terrorisme er et tema der statene må ha et vidt skjønnsrom.[89] I Klass-dommen legger domstolen til grunn at stadig økende terrorisme og grov kriminalitet fordrer nye verktøy fra myndighetenes side. Tilsvarende tankegods kan man finne i Leander-dommen. Det er dermed liten tvil om at nasjonal sikkerhet i seg selv tilsier et bredere skjønnsrom. Det fremgår av de foran nevnte dommene at statenes inngrep skal prøves uavhengig av skjønnsrommet, men at graden av rettslig prøving avhenger av hvor bredt dette er.

Det er vanskelig å definitivt konkludere uten forbehold når det gjelder trinnhøyden til interessen man søker å beskytte ved å innføre datalagringsdirektivet. Det kan synes å være slik at domstolen har en tredeling der eksplisitt definerte rettigheter i konvensjonen utgjør kjernen, et godt eksempel her er retten til respekt for korrespondanse som fremgår tydelig av art. 8. Den neste trinnhøyden består av implisitte rettigheter frembrakt av rettspraksis. Retten til en effektiv beskyttelse av liv og helse, som innbefatter effektiv etterforskning og forebygging av kriminalitet synes å være en slik. Avslutningsvis har man rettigheter og interesser som ikke er konvensjonsbeskyttet. Målet om å skape en mer demokratisk tilgang på jaktareal i Chassagnou-dommen, kan defineres på denne måten. I en slik lagdeling vil altså målet om å bekjempe grov kriminalitet falle i den andre kategorien, i motsetning til interessen direktivet griper inn i, som er eksplisitt beskyttet av art. 8. Jeg vil dog ikke legge avgjørende vekt på min tolkning av ordlyden i Chassagnou-dommen, på tross av ordlyden er sondringen domstolen foretar rettet mot en konvensjonsbeskyttet rettighet versus en rettighet som ikke er konvensjonsbeskyttet. I min problemstilling er direktivets målsetning en naturlig del av beskyttelsen art. 2 etter rettspraksis gir. Om det foreligger en forskjell på de implisitte rettigheters og de eksplisitte rettigheters natur, har jeg for få holdepunkter i rettspraksis til at jeg vil gå nærmere inn på det. Jeg antar derfor at EMD ikke vil legge avgjørende vekt på denne faktoren i bedømmelsen av hvor streng rettslig prøving domstolen bør anlegge.

For å rekapitulere vil jeg dermed legge til grunn at dette er en faktor som kan trekke litt i begge retninger. Interessen som beskyttes kan knyttes opp mot nasjonal sikkerhet i forbindelse med terrorisme og organisert kriminalitet. Dette taler for å gi statene en bred skjønnsmargin. I tillegg motiveres inngrepet av en implisitt konvensjonsbeskyttet rettighet. Samtidig er det

88 CASE OF OSMAN v. THE UNITED KINGDOM (87/1997/871/1083), §115

89 Se f.eks. CASE OF KLASS AND OTHERS v. GERMANY (Application no. 5029/71) og CASE OF LEANDER v. SWEDEN (Application no. 9248/81)

indikatorer på at implisitte rettigheter er på en lavere trinnhøyde enn eksplisitte rettigheter etter konvensjonen. Jeg vil likevel legge vekt på de to førstnevnte poengene og la denne faktoren tale for å gi statene en bredere skjønnsmargin ved en eventuell rettslig prøving av innføringslovverk.

5.2.3 Interessens målbarhet

En av faktorene EMD tradisjonelt har lagt vekt på, er hvorvidt interessen myndighetene søker å beskytte ved inngrepet er målbar. Er interessen inngrepet søker å beskytte av særs objektiv art, og sådan etterprøvbar, vil skjønnsrommet være mindre. Om interessen er av særs subjektiv art, vil skjønnsrommet være bredere. I Handyside-dommen var formålet med inngrepet av særs subjektiv art.[90] EMD kviet seg for å overprøve en skjønnsbetont moralsk beslutning, og anså de nasjonale domstolene for å være mer egnet til dette. I Sunday Times-dommen ble derimot interessen inngrepet søkte å beskytte vurdert som etterprøvbar og målbar.[91] Dette første til at skjønnsrommet ble smalere og at EMD valgte å prøve problemstillingen mer inngående. Interessen staten forsøkte å beskytte i Sunday Times-dommen, var domstolenes autoritet. Sunday Times hadde gått mot en rettsordre, og blitt straffet for dette. Motivasjonen for inngrepet var å opprettholde borgernes respekt for domstolenes autoritet. Dette ble altså ansett for å være en etterprøvbar verdi. Slik jeg tolker denne dommen er det altså ingen streng terskel for å anse noe for å være etterprøvbart/objektivt av natur. Disse to dommene kan indikere at moralske eller religiøst betonede problemstillinger av EMD blir ansett for å være lite egnet for en streng prøving.

Når det gjelder direktivet, er forebygging og etterforskning av kriminalitet målsetningen. Forskningen rundt trafikkdatas nytte, er noe mangelfull per i dag. Det er likevel klart at dette er et område det forskes på og hvor man kan analysere nytteeffekt og ulemper. Man har gjennomført intervjuer med polititjenestemenn og innhentet statistikk om innhenting som jeg har fått tilgang på både i Tyskland, Sverige, Danmark og Norge. Tilsvarende har EU selv gjennomført forskning og evaluering. Det ikke-offentliggjorte evalueringsdokumentet presenterer både kvalitative og kvantitative data fra de landene som har innført direktivet.[92] Dette indikerer at direktivmålsetningene er av en målbar art. Dette taler for en innskrenking av skjønnsmarginen ved en rettslig prøving for EMD.

5.2.4 Inngrepets natur

Det fremgår av flere dommer på dette området at inngrepets natur og intensitet tillegges vekt. Dette fremgår kanskje best i Incal-dommen.[93] Der vektlegges den radikale naturen ved inngrepet som gjøres.

90 CASE OF HANDYSIDE v. THE UNITED KINGDOM (Application no. 5493/72)
91 CASE OF THE SUNDAY TIMES v. THE UNITED KINGDOM (Application no. 6538/74) §5
92 Room Document - Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communications
93 *CASE OF INCAL v. TURKEY* (41/1997/825/1031) §56

Inngrepet datalagringsdirektivet utgjør, består av to forskjellige bestanddeler. Den første er et påbud om allmenn lagring av trafikkdata i alle offentlige kommunikasjonsnett. Dette gjelder både Internettrafikk, fasttelefoni og mobiltelefoni. Den andre bestanddelen er uthenting av disse lagrede data i forbindelse med etterforskning av grov kriminalitet. Jeg vil først se litt nærmere på det førstnevnte.

Som det fremgår av tidligere avsnitt i oppgaven, omfattes store deler av borgernes trafikkdata (i realiteten alle trafikkdata). Hvem man prater med, hvem man sender epost til og hvem man sender tekstmeldinger til. I tillegg hvor man befinner seg når man kommuniserer. I realiteten vil denne typen lagring medføre at man, spesielt om man samkjører denne typen databaser med andre databaser (skattelister, banktransaksjonshistorikk o.l.), kan få et detaljert kart over alle borgernes liv. En systematisering av denne typen data kan føre til innholdslignende konklusjoner. Et inngrep, hvis natur leder til en situasjon der lekkasjer og misbruk kan finne sted, vil sådan fremstå som mer alvorlig enn et inngrep som i mindre grad åpner for dette.

Utlevering av trafikkdata er det andre inngrepet datadirektivet gjør. Lagrede trafikkdata skal utleveres til politi- og påtalemyndigheter for bruk i etterforskning av grov kriminalitet. Dette inngrepet er av en sekundær natur, da utlevering ikke kan skje uten en forutgående lagring. Utlevering av trafikkdata isolert sett er ikke nødvendigvis et grovt inngrep. Domstolskontroll og prosedyrer for sletting av data etter endt bruk er muligheter som sikrer borgerne både mot vilkårlighet og misbruk. Såfremt denne typen sikkerhetsmekanismer innføres, vil dette inngrepet i mindre grad fremstå som problematisk i en harmoniseringskontekst. Selve lagringen av data fremstår som mer inngripende. Dette er både mer omfattende og i praksis umulig å unngå.

Slik jeg tolker rettspraksis, har det formodningen for seg at et inngrep av denne natur og intensitet taler for en streng rettslig prøving.

5.2.5 Rettigheten det gripes inn i

Det fremgår bl.a. av dette utsagnet fra Dudgeon-dommen at rettigheten det gripes inn i er relevant for vurderingen om hvorvidt et inngrep skal bli utsatt for en streng rettslig prøving:

> ”However, not only the nature of the aim of the restriction but also the nature of the activities involved will affect the scope of the margin of appreciation. The present case concerns a most intimate aspect of private life. Accordingly, there must exist particularly serious reasons before interferences on the part of the public authorities can be legitimate for the purposes of Article 8 (2).”[94]

Hva slags rettighet det gripes inn i og hvordan, står altså sentralt i vurderingen av hvor streng den rettslige prøvelsen fra EMD vil bli.[95] Det er flere dommer som indikerer at EMD plasserer rettighetene i et hierarki. Dudgeon-dommen omhandler et særs subjektivt vurderingstema (offentlig moral, dommen omhandlet homoseksuelt samliv og sanksjoner mot dette).[96] Denne typen vurderingstema har EMD tradisjonelt latt statene gjøre med et forholdsvis stort

94 CASE OF DUDGEON v. THE UNITED KINGDOM (Application no. 7525/76)
95 Se bl.a. CASE OF LINGENS v. AUSTRIA (Application no. 9815/82
96 Se f.eks. CASE OF DUDGEON v. THE UNITED KINGDOM (Application no. 7525/76)

spillerom. Reguleringer av utpreget moralsk/subjektiv natur (skilsmisseregler, regler for homoseksuelt samliv, religionspolitikk) har tradisjonelt blitt lite strengt prøvet av EMD. I Dudgeon-dommen gikk det motsatt vei. EMD sier i denne dommen at på tross av det utpregede moralske vurderingstemaet, så kan ikke inngrepet anses for å være i samsvar med EMK. Begrunnelsen for dette er at homoseksuelt samliv utøvd i det private, er helt i kjernen av det personlige og private. Hvis staten vil gripe inn i hva borgerne gjør innenfor hjemmets fire vegger, kreves særskilt gode grunner.

Slik jeg tolker uttalelsen fra dommen over, må det spesielt gode grunner til å gripe inn, hvis inngrepet foretas i forhold til de mest intime deler av privatlivet. Dette legger en videre føring på fastsettelsen av det skjønnsrommet statene har i forhold til inngrep. Hva som utgjør det "most intimate aspect of private life" er ikke enkelt å avgrense skarpt. I denne dommen er det snakk om seksuelle relasjoner mellom mennesker av samme kjønn i sitt eget hjem. Det er naturlig å anta at forhold som gjelder seksualitet, privat religionsutøvelse i hjemmet o.l. vil falle inn under denne paraplyen. Støtte for dette synspunktet finner man også i Connor-dommen, der EMD sier bl.a. dette:

«The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights»

Slik jeg tolker denne uttalelsen, vil en rettslig prøving på et område der nøkkelrettigheter eller intime rettigheter resultere i en strengere rettslig prøving. Dette er en faktor som kan gjøre seg gjeldende for vurderingstemaet i min oppgave. Flere forhold som kan bli omfattet av datalagringsdirektivet i sin nåværende form, kan være elementer av intime deler av ens liv. Eksempler på dette er helseopplysninger og andre personlige forhold (kommunikasjonsdata relatert til oppringninger til en HIV/AIDS-klinikk f.eks.) eller kontakt med telesextjenester eller lignende. Mindre intuitivt, men kanskje enda viktigere, er informasjonen man kan hente ut med såkalt data-mining. Dette er opplysninger man kan få ved å systematisere enkelte brukeres trafikkdata.[97] Undersøkelsen fra MiT viser at man kan hente ut store mengder informasjon fra trafikkdata i systematisert form.

Jeg vil også peke på uttalelser i Kruslin-dommen:

> "Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence [...]"[98]

Avlytting og andre former for kommunikasjonskontroll blir eksplisitt beskrevet som et alvorlig inngrep i privatliv og korrespondanse. Jeg kan ikke se noen grunn til ikke å applisere disse uttalelsene også på Internettbasert kommunikasjon.

97 MiT, 2009, http://reality.media.mit.edu/dyads.php
98 Case of Kruslin v. France *(Application no. 11801/85)*

Et lignende prinsipp fremgår av Lingens-dommen, her blir det understreket at pressen, og det bidrag pressen gir til en god offentlig debatt er uvurderlig, og at frie meningsutvekslinger er en gjennomgående kjerneverdi i den formen for moderne demokrati som konvensjonen ønsker å opprettholde. Man kan argumentere for at fri kommunikasjon både med gamle og nye kommunikasjonsmidler også vil falle nært denne kjernen i konvensjonen. Mer spesifikt er det spesielt to momenter som taler for å legge interessene det gripes inn i, sentralt i konvensjonen.

For det første kan man peke på Internettfora og nye former for organisering både nasjonalt og internasjonalt. Stadig større deler av den frie politiske diskurs, meningsdannelse og meningsytringer foregår på åpne eller lukkede Internettforum. Spesielt fremtredende i denne kontekst er mange autoritetskritiske grupperinger og organisasjoner som spesialiserer seg på myndighetskritikk og varsling. Man kan bare se på den posisjon Wikileaks har etablert på noen få år, for å forstå hvor viktig slike organisasjoner har blitt i moderne politikk. Man kan f.eks. se på en av de senere Wikileaks-sakene.[99] Saken fikk enorm publisitet og skapte et internasjonalt press på USA og førte til utenrikspolitisk etterspill. Denne typen organisasjoner er avhengig av å beskytte kilder mot myndighetene/organisasjonene de lekker fra, og i enda større grad enn ordinær presse er de avhengige av et effektivt og vanntett kildevern. Direktivet griper direkte inn i dette og har en potensielt kjølende effekt på denne typen organisasjoner og deres drift. Dette skisserer for øvrig en annen problemstilling EMD ennå ikke har tatt stilling til, at grensen for hva som kan anses for å være «presse» blir stadig mer flytende. Er Wikileaks journalister? Kan de omfattes av kildevernet? Dette er spørsmål som tangerer min problemstilling. Det er dog ikke rom for denne typen vurderinger i min oppgave.

For det andre er det i direktivet ikke tatt høyde for at tradisjonelt beskyttede kommunikasjonsformer, pressens kildevern, forholdet til advokaters kommunikasjon med sine klienter og lignende skal vernes. Dette har også en potensiell negativ effekt på pressens tilgang på anonyme kilder. EMD legger vekt på at pressens kildevern må beskyttes, dette er gjennomgående i rettspraksis. Lignende problematikk oppstår når det gjelder trygghet rundt detaljer om helsedata. Som EMD understreker i Monory-dommen, skal slike data beskyttes.[100] Systematisering av trafikkdata vil som sagt kunne avsløre mye om borgernes situasjon på dette området.

Hvorvidt disse potensielle problemene vil aktualiseres, er vanskelig å si, men at direktivet vil kunne ha en potensiell avkjølende virkning på flere viktige samfunnsfunksjoner, må man kunne legge til grunn slik jeg tolker situasjonen og de foreliggende data. Derfra er det, i lys av rettpraksis, og da spesielt uttalelsene i Lingens-dommen, naturlig å gå til det skritt å legge rettighetene direktivet griper inn i, nært kjernen av konvensjonen. Dette taler for at EMD vil å prøve en innføring av direktivet strengt.

99 Wikileaks, 2010, http://www.guardian.co.uk/world/2010/apr/05/wikileaks-us-army-iraq-attack
100 CASE OF MONORY v. ROMANIA AND HUNGARY (Application no. 71099/01)

5.2.6 Konklusjon

Etter dette, har det formodningen for seg at EMD vil underlegge direktivet en forholdsvis streng rettslig prøving. Både det faktum at direktivet angår nasjonal sikkerhet og at rettigheten det gripes inn til fordel for er en implisitt konvensjonsbeskyttet rettighet, taler for en større skjønnsmargin for statene. Samtidig er rettigheten det gripes inn i en eksplisitt rett/kjernerettighet, retten det gripes inn til fordel for er en objektivt målbar interesse, inngrepet er av en særlig omfattende natur og overvåkningsområdet er tradisjonelt et område hvor EMD har valgt å gi statene en smal skjønnsmargin. Jeg vil i de videre vurderinger legge dette til grunn.

5.3 Proporsjonalitets – og nødvendighetsvurderinger

5.3.1 Innledning

I forrige kapittel prøvde jeg å belyse hvorvidt EMD vil gi statene en bred eller smal skjønnsmargin når det gjelder innføringen av direktivet. Min konklusjon ble der at EMD mest sannsynlig vil utsette en direktivinnføring for en streng rettslig prøving. Det innebærer at de proporsjonalitets- og nødvendighetsvurderinger som kommer i det videre, vil innebære en streng terskel.

Dette er den viktigste problemstillingen i min oppgave. Er datalagringsdirektivet et nødvendig og proporsjonalt inngrep i retten til respekt for privatliv og korrespondanse? Kan man harmonisere de krav direktivet stiller til medlemsstatene i EU og EØS om lagring og de krav EMK art. 8 stiller når statene skal gjøre unntak fra hovedregelen?

Inngrep i rettighetene gitt med hjemmel i EMK art. 8, må være nødvendige. Dette fremgår av ordlyden i andre ledd. Jeg vil ta utgangspunkt i ordlyden, drøfte hvordan rettspraksis har utviklet begrepet, for så å gå gjennom forskjellige momenter av direktivet. Den første delen av kapittelet vil være teoretisk, der jeg vil forsøke å redegjøre for det rettslige grunnlaget for proporsjonalitetsvurderingen. I resten av kapittelet vil jeg forsøke å bruke dette på de foreliggende fakta.

Vurderingstemaene under hovedproblemstillingen nevnt over, er flere. Jeg vil derfor se på de enkelte gjennomføringselementene, finnes det bedre alternativer? Hvilke konsekvenser får forskjellige deler av innføringen? Er dette en stor endring fra den bestående ordning? Hvor stor samfunnsnytte har man av direktivet?

Det meste av dette kapittelet vil bli preget av at jeg må ta en del forbehold. EMDs praksis på dette området fører sjelden til allmenngyldige prinsipper, og de begrunnelser som foreligger gir rom for flere tolkninger. Videre er også det datagrunnlag jeg har i forhold til kriminalitetsbekjempelse, konsekvenser av direktivet o.l. begrenset og preget av mulige feilkilder. Disse to faktorene, blant flere, gjør det vanskelig å presist forutse EMDs reaksjon på de forskjellige implementeringslover, noe som gjør at jeg må uttale meg med forsiktighet. I

tillegg kan det være verdt å gjenta at jeg ikke har en konkret gjennomføring jeg kan holde opp mot de prinsipper jeg destillerer fra rettspraksis.

5.3.2 Rettslig grunnlag for proporsjonalitetsvurderingen

Innbakt i EMK artikkel 8 er det et nødvendighetskrav. Ordlyden gir liten veiledning for hva som ligger i dette. Hva er nødvendig, hvordan skal man avgrense begrepet? Dette kravet har gjennom rettspraksis blitt utviklet fra å være en vidt formulert, til å få et mer definert innhold gjennom rettspraksis. Jeg vil gå gjennom de forskjellige faktorene som blir vektlagt i nødvendighetsvurderingen i rettspraksis.

EMD uttalte tidlig, i Handyside-dommen dette:

> ”The Court notes […] that, while the adjective ’necessary’ […] is not synonymous with ’indispensable’, neither has it the flexibility of such expressions as ’admissible’, ’ordinary’, ’useful’, ’reasonable’ or ’desirable’”[101]

Det er altså ikke snakk om at de inngrep som gjøres må være helt uunngåelige eller essensielle for samfunnets videre funksjon. Ei heller er det snakk om at inngrep kan aksepteres fordi de er nyttige, ønskelige, rimelige eller av lignende hensyn. Dette presiserer ordlyden i konvensjonen ytterligere.

Det neste ledd i utviklingen kom i Olsson-saken. Der sier EMD:

> ”According to the Court’s established case-law, the notion of necessity implies that an interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued”[102]

Det fremgår her at nødvendighetsprinsippet innebærer at det må foreligge et presserende sosialt behov for det inngrepet som gjøres, og at inngrepets legitime mål og dets resultater må være proporsjonale i forhold til inngrepet som gjøres og de konsekvenser det får. Her spesifiseres prinsippene fra Handyside-dommen ytterligere, og man får en ytterligere presis mal for proporsjonalitetsvurderingen. Man har nå rommet mellom “pressing social need” og “indispensible” hvor statene kan bevege seg. Det ekskluderer mange inngrep som utgjør et nyttig bidrag til f.eks. politi- og påtalemyndigheter, men som ikke tilsvarer et presserende sosialt behov. Dette inntrykket forsterkes av uttalelser i Klass-dommen:

> «Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.»

Her fremgår det at overvåkningstiltak kun kan aksepteres i den grad de er strengt nødvendige for å sikre de demokratiske institutsjoner. Dette gjelder dog innholdsovervåkning, men som jeg kommer inn på flere steder, er grensen mellom innholdsdata og trafikkdata i stadig større

101 Handyside v. Uk, 1976

102 Olsson v. Sweden, 1988)

grad flytende. Man kan trekke mange innholdslignende konklusjoner fra trafikkdata. Min tolkning av rettspraksis indikerer at EMD vil anlegge en streng terskel for nødvendighetsvurderinger rundt det inngrepet direktivet utgjør.

Et annet poeng som kan være verdt å merke seg før man begir seg ut på den videre proporsjonalitetsvurderingen, er domstolens tendens til å foreta svært konkrete vurderinger, uten å utdype videre om hva landene kunne ha gjort verken i positiv eller negativ forstand for å kommet nærmere en hypotetisk terskel, eventuelt over denne. Det er dermed vanskelig å utkrystallisere noen allmenne prinsipper fra rettspraksis når det gjelder proporsjonalitetsvurderingen. Dette blir omtalt i detalj av Hutchinson.[103] Derfor er det tildels vanskelig å lage en presis fremgangsmåte eller mal for proporsjonalitetsvurderingen, og at man i stor grad må lene seg på de fremtredende fordeler ved et inngrep og vurdere disse konkret, både enkeltvis og samlet, opp mot de ulemper inngrepet medfører. Dette fremgår også bl.a. av Sunday Times-dommen. Denne dommen er et godt eksempel på den konkrete og spesifikke natur en slik nødvendighetsvurdering vil ha. Dette gjør vurderingen av potensielle inngrep i form av generelle lovverk vanskeligere. Det er dog noen vurderingstema som går igjen, jeg vil se nærmere på disse i det følgende.

Et moment EMD tradisjonelt har vurdert, er potensielt alternative handlemåter. Av Blecic-dommen fremgår det at alternative, mindre inngripende handlemåter i seg selv ikke er avgjørende, men at dette er et moment som må tas med i en helhetsvurdering rundt proporsjonalitet.[104] Er det alternative handlemåter som ville ledet til tilsvarende beskyttelse i forhold til inngrepets målsetning og disse er av en mindre inngripende natur, er dette selvsagt en tungtveiende faktor. Er det derimot større forskjell på måloppnåelse og mindre forskjell når det gjelder inngrepets natur, er det naturlig å tillegge dette momentet mindre vekt. Det er naturlig å bringe dette inn i den videre drøftelse flere steder i det følgende, da flere forskjellige deler av direktivet kan sies å ha alternativer verdt å drøfte. Annderledes blir et når et inngrep ikke forandrer situasjonen eller man kunne endt opp med det samme resultatet uten å utføre inngrepet. Dette fremgår klarest av Monory-saken.[105] Her sier EMD det at man kunne endt opp med samme resultat, uten å ty til inngrepet som ble gjort. Her ble altså inngrepets manglende betydning for sluttresultatet avgjørende.

Videre drøftes inngrepets potensielle konsekvenser for samfunnet som helhet, samt for de som utsettes for inngrepet. Dette fremgår bl.a. av Klass-dommen.[106] Hvis et inngrep potensielt kan føre til en forringelse av demokratiet, er dette noe som tillegges stor vekt av EMD. Jeg vil se nærmere på hvilke konsekvenser direktivet tildels har hatt og tildels potensielt kan ha på forskjellige samfunnsområder.

Jeg vil også se på hvilken nytte samfunnet har av inngrepet. Dette er et sentralt moment i proporsjonalitetsvurderingen og er i mange saker avgjørende. Det er mange eksempler i

103 Hutchinson, 2008
104 CASE OF BLECIC. CROATIA (Application no. 59532/00) §67
105 CASE OF MONORY v. ROMANIA AND HUNGARY (Application no. 71099/01)
106 CASE OF KLASS AND OTHERS v. GERMANY (Application no. 5029/71)

rettspraksis på at domstolen legger vekt på inngrepets nytteeffekt.[107] En komponent av denne vurderingen, er at behovet for inngrepet "must be convincingly established.".[108] Dette avsnittet vil dermed gå gjennom både en generell samfunnsnytte, men også spesifikt gå gjennom hvorvidt denne samfunnsnytten møter de krav til sosialt presserende behov rettspraksis fra EMD reiser. Tilsvarende vil jeg også gå gjennom hvorvidt behovet for direktivet var tilstrekkelig overbevisende klargjort før det ble vedtatt og innført.

Avslutningsvis vil jeg se på hvorvidt det har blitt etablert gode sikkerhetsmekanismer i forbindelse med direktivet. I forrige kapittel gikk jeg gjennom sikkerhetsmekanismer som en del av lovkvalitetsspørsmålet, men bl.a. Leander-dommen viser at sikkerhetsmekanismer også er et moment EMD legger vekt på ved proporsjonalitetsvurderingen.

5.3.3 Konsekvenser av datalagringsdirektivet

Problemstillingen jeg skal se nærmere på her, er hvilke konkrete konsekvenser direktivet har. Dette er en viktig faktor i proporsjonalitetsdrøftelsen. Hvilke konsekvenser det har for borgernes kommunikasjonsmønstre at alle trafikkdata lagres? Hvilke konsekvenser har det for øvrig? Jo større ringvirkninger direktivet har, jo sterkere må begrunnelsene for direktivet være for å muliggjøre en harmonisering. Dette er en av drøftelsene i dette kapittelet jeg må ta størst forbehold, da det til nå foreligger få undersøkelser i de land som har innført direktivet.

Jeg vil først se nærmere på en undersøkelse om nettbruk i forbindelse med direktivet gjort i Tyskland, videre vil jeg drøfte potensielle negative konsekvenser for pressen. Dette er en faktor EMD tradisjonelt har tillagt stor vekt. Et godt eksempel på dette er Sanoma Uitgevers-dommen der etterforskning av grov kriminalitet blir underordnet hensynet til pressens kildevern.[109] Retten understreker her gjentatte ganger alvoret i å foreta inngrep som kan føre til en nedkjøling av pressens aktivitet. Avslutningsvis skal jeg se på noen problemstillinger med såkalt "mission creep". Før jeg går inn på de enkelte momentene vil jeg bare gjenta EMDs syn på personlige data. Det kommer kanskje spesielt klart frem i Monory-dommen, der domstolen understreker at respekt for personlige info er essensielt. Tilsvarende kommer frem i Klass-dommen:

> "... a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole..."[110]

EMD understreker her hvor viktig det er å vurdere konsekvensene, både potensielle og aktuelle, for det demokratiske samfunn når det gjelder overvåkning. Det kan også være verdt å gjenta at grensen mellom trafikkdata og innholdsdata blir mer og mer flytende jo mer avansert teknologien blir. Vi bruker en stadig større flora av løsninger for å kommunisere med

107 CASE OF FUNKE v. FRANCE (Application no. 10828/84)
108 CASE OF FUNKE v. FRANCE (Application no. 10828/84)
109 CASE OF SANOMA UITGEVERS B.V. v. THE NETHERLANDS (Application no. 38224/03)
110 CASE OF MONORY v. ROMANIA AND HUNGARY(Application no. 71099/01)

hverandre og i mange tilfeller kan man hente mer informasjon ut av trafikkdata enn man kan av innholdsdata. Dette medfører at å bruke en skarp avgrensning mellom trafikkdata og innholdsdata blir lite reelt slik jeg ser det. Tradisjonelt har EMD lagt faktiske, og ikke formelle forhold til grunn, dette tror jeg nok også vil være tilfellet her.

Det første faktoren jeg vil se nærmere på, er Forsa-undersøkelsen fra Tyskland.[111] De tallene man bør merke seg er at det i den korte perioden datalagringsdirektivet var aktivt i Tyskland, var det 11 prosent som allerede hadde endret sine kommunikasjonsmønster som en reaksjon på direktivet. I tillegg svarte 55 prosent at de ville unnlate å foreta sensitiv kommunikasjon ved hjelp av elektroniske kommunikasjonsmidler i fremtiden. Som tidligere nevnt, er elektronisk kommunikasjon en sentral del av et moderne demokrati. Et godt eksempel på dette er det pågående prosjektet "The Internet and Democracy Project" fra Harvard, der man kartlegger kommunikasjonsvaner og søker å styrke fokus på Internett og andre kommunikasjonsformer som viktige demokratiske verktøy. Tilsvarende kan man finne flere forskere som peker på at Internett bidrar til økt politisk og demokratisk deltagelse samt økt sosial mobilitet.[112] Datagrunnlaget jeg sitter på er forholdsvis smalt, likevel vil min hypotese være at direktivet generelt sett vil medføre endrede kommunikasjonsvaner. Spesielt gjelder dette omstridte politiske grupperinger og sensitiv kommunikasjon. Det har formodningen for seg at grupperinger som blir ansett som uønsket (ekstreme rasister, autonome/anarkistiske grupperinger, fundamentalistiske religiøse grupperinger) vil endre kommunikasjonsmønster, videre synes også å være naturlig å dra den slutning at befolkningen forøvrig vil begrense sine ytringer på Internett og sin endre sine kommunikasjonsvaner når det gjelder sensitive forhold. Det er vanskelig å kvantifisere betydningen av dette, spesielt da det empiriske grunnlaget er begrenset. Likevel kan det være verdt å peke på at EMD tradisjonelt sett har ansett fri meningsdannelse og uhindret politisk virksomhet som kjerneverdier, og at disse, om enn vage, verdiene vil veie tungt i en eventuell vurdering fra domstolens side.

Det andre momentet, som er enklere å drøfte i en rettskildekontekst, er forholdet til pressens kildevern. Jeg har så vidt gått inn på dette i kapittelet om lovkvalitet, men det er også relevant i forhold til hvordan direktivet innvirker på samfunnet. EMD har ofte vært kritisk til inngrep som kan føre til en nedkjøling av pressens rolle som samfunnsaktør. I Uitgevers-saken, som nylig var oppe for EMD, understreker EMD ytterligere hvor viktig pressens kildevern er for en kritisk og informert presse.[113] Saken gjaldt politiets ønske om å få utlevert kildeinformasjon, ikke for å straffeforfølge eller identifisere kildene, men for å få ut informasjon i forbindelse med en annen sak. Denne andre saken blir beskrevet som grov. Likefullt anså EMD inngrepet for å være uønsket i lys av hvor sentralt pressens kildevern er. Uten tillit til at pressens kildevern er absolutt, vil varslere og anonyme kilder i langt større grad vegre seg for å gi ut viktig informasjon til pressen. Dette er i all hovedsak problemstilling relatert til artikkel 10. Jeg velger likevel å drøfte det her, da direktivet har potensielle konsekvenser for pressens kildevern. Som tidligere nevnt har EMD lagt stor vekt på å unngå inngrep som kan kjøle ned den frie presse. Det er, som jeg klargjorde over, svært

111 Meinungen der Bundesburger zur Vorratsdatenspeicherung - Gesekkschaft fur Sozialforschung und statistische Analysen mbH, en spørreundersøkelse fra Tyskland der man spurte borgerne om kommunikasjonsvaner og mulige endringer som følge av direktivinnføring, 2008, http://www.eco.de/dokumente/20080602_Forsa_VDS_Umfrage.pdf

112 Jones, 1997, Virtual Culture: Identity and Communication in Cybersociety

113 CASE OF SANOMA UITGEVERS B.V. v. THE NETHERLANDS (Application no. 38224/03)

vanskelig å bruke tekniske virkemidler for å unngå at trafikkdata fra journalisters kommunikasjon blir lagret. Man må dermed forutsette at også denne typen data vil bli lagret og sikre at disse ikke blir brukt ved domstolsbehandlingen. Dette sikrer mot vilkårlige inngrep fra politi- og påtalemyndighet. Det er derimot ikke en sikkerhet mot ulovlig eller ureglementert tilgang på data når de lagres hos leverandører. Det er vanskelig å kartlegge hvor stor sannsynlighet det er for lekkasjer og misbruk. Vi har hatt trafikkdata lagret hos leverandørene de siste 15år, uten at større skandaler har nådd offentlighetens lys. Dette kan indikere at problemet ikke nødvendigvis vil oppstå med innføring av direktivet. Man kan dog ikke se bort fra at det har vært episoder hvor trafikkdata har lekket uten at noen av de involverte aktørene har ønsket en offentliggjøring. Teknologiske fremskritt og nye kommunikasjonsvaner vil også føre til at trafikkdata utgjør en viktigere kilde til informasjon. Stadig flere tjenester og stadig mer frekvent kommunikasjon gjør at man får et mer og mer komplett bilde av kommunikasjons- og reisevaner. Jeg har ikke nok data tilgjengelig til at jeg vil komme med noen renskårne konklusjoner rundt farene for lekkasjer. Slik jeg ser det er det likevel verdt å nevne denne problemstillingen. Dette kan være et problem i forhold til en harmonisering av datalagringsdirektivet og EMK.

Tilsvarende problemstillinger oppstår i relasjon til kommunikasjon mellom advokater og deres klienter. Hvis det er praktisk umulig å unngå lagring av trafikkdata for slik kommunikasjon, vil det også her foreligge utvidet lagring her i forhold til hva som har vært praksis. Som det fremgår i Iordachi-saken, kan dette være problematisk.[114] Et minstekrav i forhold til EMK er at man har et klart regelverk som regulerer denne typen kommunikasjon:

> "The Court is struck by the absence of clear rules defining what should happen when, for example, a phone call made by a client to his lawyer is intercepted."

Også her synes jeg det er vanskelig å konkludere. Hvis det er umulig å regulere lagring av trafikkdata fra vernede grupperinger, er det lite sannsynlig at dette blir påbudt. Da blir dette i større grad en vurdering rundt proporsjonalitet.

En annen problemstilling jeg vil drøfte under dette punktet, er såkalt "mission creep". Direktivets offisielle formål er todelt. Bekjempelse av grov kriminalitet og harmonisering av lagrings- og slettingsregler for ekomleverandører. En problemstilling er å avgjøre om dette formålet indikerer et minstekrav, slik at statene selv kan utvide bruksområdene for lagrede data. Alternativet er at direktivet setter som krav at data kun kan brukes til det eksplisitte formålet. Slik jeg tolker ordlyden i direktivet, er det noen eksplisitte påbud i direktivet. Bl.a. lagringstid, krav til evaluering og statistikk. Derimot kan jeg ikke ut fra ordlyden anse bruksområdene for trafikkdata for å være låst til de hovedformål direktivet dikterer. I forhold til direktivet er det dermed ikke i utgangspunktet et problem at bl.a. Storbritannia har valgt å tillate bruk av trafikkdata i sivile søksmål.[115] Det er derimot en faktor når man skal drøfte hvorvidt direktivet er proporsjonalt eller ikke. Et utvidet bruksområde gir en utvidet nytteeffekt. Dette taler til fordel for direktivet. På den andre side, utgjør dette et større inngrep i forhold til borgerne. At ens trafikkdata kan brukes i forbindelse med grov kriminalitet vil nok møte langt større aksept enn om trafikkdata også kan brukes som bevis i skilsmissesaker, erstatningssaker o.l. Et godt eksempel på hvordan dette nok ville bli oppfattet av publikum,

114 CASE OF IORDACHI AND OTHERS v. MOLDOVA (Application no. 25198/02) - §§48-50

115 Evaluation of directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communication

fikk vi i den nylige NAV-overvåkningssaken.[116] En stille lovendring førte til at NAV fikk tilgang, uten søknad eller øvrige begrensninger, på borgernes trafikkdata. De reaksjonene som kom, indikerer at dette ble oppfattet som et langt mer alvorlig inngrep enn politiets tilgang.

Dette kan indikere at det er vanskeligere å anse direktivet som nødvendig og proporsjonalt, om det innebærer at trafikkdata kan brukes som bevis i sivile saker. Klass-saken underbygger dette poenget der fremgår det at overvåkning bør skje:

> "in the interests of national security and/or for the prevention of disorder or crime."[117]

Bruk av overvåkningsdata i forbindelse med sivile saker, faller ikke inn under disse kategoriene. Sitatet har noe mindre vekt, da dette ikke var hovedproblemstillingen i saken. Jeg har likevel valgt å inkludere det, da det belyser det problematiske ved å la overvåkningsdata bli brukt i sivile saker. Det kan være nærliggende å anta at en forutsetning for en harmonisering mellom direktivet og EMK er innøfringslover som sikrer at trafikkdata kun brukes i forbindelse med straffesaker.

Avslutningsvis vil jeg peke på faren for lekkasjer og misbruk av trafikkdata. Organisasjonen Wikileaks har satt denne problemstillingen på kartet for alvor den siste tiden med gjentatte lekkasjer av hemmelige data. Dette er informasjon som spenner fra hemmelighetsstemplet diplomatkommunikasjon til hemmelige dokumenter fra krigen i Irak. Tilsvarende kan man peke på de mange datasikkerhetsskandalene i regjeringskvartalet det siste året, der det bl.a. har blitt avdekket store datalekkasjer fra regjeringens lokaler. Dette er alle indikatorer på at datasikkerhet er et vanskelig felt hvor mulighetene for lekkasjer og misbruk er mange. Det er flere problemstillinger man kan se nærmere på i så måte.

De siste årene har det ikke vært noen offentlige skandaler knyttet til lekkasjer av trafikkdata. Dette er ikke nødvendigvis en indikator på at det ikke har skjedd, men trafikkdata har ikke blitt verifisert lekket. Årsakene til dette kan være flere. Trafikkdata er lagret spredt og i mange forskjellige formater, man må sådan komme seg inn i en rekke forskjellige systemer og tilgjengeliggjøre dataene for å bruke dem på illegale måter. Videre har det først de siste 5-10 år vært en eksplosjon i mobil- og Internettkommunikasjon, så dette er et forholdsvis nytt konsept. Det er også potensielle endringer som kan føre til at dette forandres. For det første kan en løsning ved innføring av direktivet føre til at leverandørene har to databaser, hvorav den ene er en ferdig vasket (tilgjengeliggjort) database med de data direktivet påbyr. Dette samtidig med ordinær forretningsbasert lagring i en annen database. Dette gjør at trafikkdata potensielt kan bli lettere tilgjengelige rent programvaremessig. Videre vil det også bli lagret trafikkdata lengre, noe som øker sannsynligheten for misbruk og samtidig gjør konsekvensene ved lekkasjer større.

Forsvarsdepartementet viser også til problemer med misbruk og lekkasjer i sin høringsuttalelse.[118] De understreker spesielt faren ved at såkalte trusselaktører kan få tilgang på bevegelsesmønster og kommunikasjonsmønster tilhørende sentralt personell. Dette utgjør

116 http://www.dagbladet.no/2010/11/20/nyheter/innenriks/nav/datalagring/14367972/ - NAV har lov til å spionere på deg - Kan få utlevert alle dine sensitive trafikkdata, noe politiet bare kan drømme om..

117 CASE OF KLASS AND OTHERS v. GERMANY (Application no. 5029/71)

118 Høring om Datalagring, 14. april 2010, Forsvarsdepartementet

ifølge Forsvaret en reell risiko. Forsvaret etterlyser i sin konklusjon videre utredninger av informasjonssikkerhet.

Jeg vil kort vise til et prosjekt fra MIT der man ser på hvilke typer informasjon man kan hente ut fra trafikkdata.[119] Her fremgår det at man med veldig høy grad av sannsynlighet kan forutse hvem man omgås med sosialt, hvem man jobber med og hvor man kommer til å være på et gitt tidspunkt kun ved hjelp av trafikkdata. I de fleste tilfellene kunne forskerne forutse denne typen informasjon med en sikkerhet på mer enn 90%. Dette indikerer at trafikkdata er en kilde til informasjon med forholdsvis stor detaljgrad. De datahøstingsalgoritmene som her brukes er i en enorm utvikling og man kan i stadig mer presis grad hente ut personlig informasjon av stadig mer komplekse trafikkdata. Det at både teknologien for analyse av trafikkdata og trafikkdatas detaljgrad øker, har en kumulativ effekt. Resultatet er at man med økende presisjon kan kartlegge hvem noen har i sin vennekrets, hvem noens kolleger er, hva disse liker å gjøre og når de liker å gjør det. Dette underbygger de ankepunktene Forsvarsdepartementet setter søkelyset på i forbindelse med informasjon om sentralt personell. Slik jeg ser det er dette en faktor EMD vil vektlegge i en vurdering. Det at man i så stor grad kan kartlegge menneskers liv og omgangskrets ved hjelp av trafikkdata, indikerer at skillet mellom trafikkdata og innholdsdata i økende grad viskes ut. Slik jeg ser det, vil nok dette lede til strengere terskler for også denne typen overvåkning.

Det er vanskelig å si noe avgjørende om hvor stor fare det er for misbruk. Samtidig kan man nesten garantere at datalekkasjer vil skje, spørsmålet er bare om i hvilken utstrekning og hva konsekvensen kan og vil være. Hvis noen bryter seg inn i flere databaser vil de kunne lage svært detaljerte bilder om bevegelses- og kommunikasjonsmønster som kan brukes til forskjellige formål. Uten å konkludere skarpt vil jeg understreke at dette er et argument som taler merkbart i disfavør for en harmonisering av direktivet og EMK. Hvis man ikke kan gjennomføre direktivet uten å øke risikoen for lekkasjer og muligheten for at kriminelle eller

119 http://reality.media.mit.edu/dyads.php

andre aktører kan få systematisk oversikt over nøkkelborgeres kommunikasjons- og reisevaner, er dette EMD sannsynligvis vil tillegge vekt.

5.3.4 Allmenn lagring av data

Jon Wessel-Aas hevder i sitt bidrag til en ny bok om overvåkning at den allmenne lagringen av trafikkdata i seg selv er hovedproblemet.[120] Wessel-Aas peker bl.a. på Weber and Saravia v. Germany[121] og Liberty and others v. UK[122] og hevder at disse underbygger et krav om individuell begrunnelse/behandling av hvert enkelt overvåkningstiltak. I disse sakene ble Internettrafikk fra og til utlandet gjennomsøkt med utgangspunkt i søkeord som skulle sile ut mistenkelig kommunikasjon. Tysklands inngrep ble godkjent på bakgrunn av at søkevilkår var klart definerte og relaterte til de lovbrudd inngrepet søkte å bekjempe. I tillegg var det en hel rekke sikkerhetsmekanismer hvis formål var å unngå vilkårlige inngrep og misbruk. Englands inngrep ble derimot ikke godkjent, da skjønnsrommet som ble gitt myndighetene i relasjon til valg av søkeord var for vidt og prosedyrer for lagring, bruk, deling og sletting ikke var tilgjengelige.

Weber and Saravia-dommen kan tolkes dit hen at den krever at overvåkningstiltak skal via søkeord eller andre metoder og teknikker, rettes mot en avgrenset gruppe mennesker. EMD sier det slik:

> «a series of restrictive conditions had to be satisfied before a measure entailing strategic monitoring could be imposed»

En slik tolkning vil gjøre en harmonisering av EMD og datalagringsdirektivet umulig. Det er dog forskjeller på denne typen overvåkning og lagringen av trafikkdata. Den viktigste forskjellen er det den åpenbare forskjellen på trafikkdata og innholdsdata. Som nevnt over er denne forskjellen i stadig mindre grad markant. Dette kan føre til at uttalelsene i denne dommen med større tyngde kan anvendes også på trafikkdata i fremtiden

Jeg synes det er for mange usikkerhetsmomenter til å konkludere skarpt her. Mange teoretikere synes dog å anse dette som den største problemstillingen for en harmonisering av datalagringsdirektivet og EMK. Wessel-Aas er blant disse og avslutter vurderingen her. Jeg velger å drøfte øvrige problemstillinger ved harmoniseringen i det videre.

5.3.5 Samfunnsnytte og behov

5.3.5.1 Innledning

I denne delen av oppgaven, skal jeg se nærmere på hvilken samfunnsnytte direktivet har. Hvor stort er behovet for direktivet, og i hvor stor grad kan direktivet slik det fremstår i dag, møte dette behovet? De studier og det øvrige datagrunnlag jeg har, er av en slik natur at det er vanskelig å konkludere. Jeg vil likefullt prøve å belyse forskjellige sentrale problemstillinger. Jeg har tidligere i oppgaven pekt på forskjellige studier der man har søkt å finne hvor stor

120 Overvåkning i en rettsstat, Dag Wiese Schartum, Fagbokforlaget 2010
121 Ikke-publisert.
122 CASE OF LIBERTY AND OTHERS v. THE UNITED KINGDOM (Application no. 58243/00)

nytte politiet har av trafikkdata som etterforskningsverktøy, jeg vil se på disse litt nærmere. Jeg vil også se på den praksis jeg har fått tilgang på fra medlemsland som har innført direktivet. Her er det noen statistiske momenter som kan være verdt å ta med seg videre. I denne forbindelse vil jeg også se litt på det forhold at trafikkdata er et verktøy politiet har hatt tilgang på i 15-20 år, og at direktivet tildels opprettholder dette ved å påby lagring. Jeg vil avslutningsvis se litt på hvorvidt de data man har fra dagens praksis med Post- og teletilsynet kan være en indikator på fremtidig bruk i Norge under datalagringsdirektivet.

5.3.5.2 Tall fra politiet

Jeg vil her søke å skissere hvilken nytte politiet har av trafikkdata i sin etterforskningshverdag.

Jeg har tidligere pekt på flere studier fra bl.a. Norge og Sverige som baserer seg på intervjuer med polititjenestemenn.[123] Her fremgår det at politiet anser trafikkdata som et nyttig verktøy i underkant av halvparten tilfellene der de får disse data utlevert. Undersøkelsene er dog binære av natur, det er ingen andre svar enn "nyttig" og "ikke nyttig" slik jeg har forstått dem, det gjør at det er vanskelig å trekke klare konklusjoner fra disse tallene. "Nyttig" kan bety alt fra en mindre positiv innflytelse til avgjørende viktighet, og spenner sådan over et stort spekter. I løpet av debatten den siste tiden har det kommet flere uttalelser fra sentrale polititjenestemenn om nytten av trafikkdata som bevis, denne uttalelsen fra KRIPOS-sjef Odd Reidar Humlegård er i så måte betegnende:

> "I dag er trafikkdata et basisverktøy, et verktøy vi ikke lenger greier oss uten - på linje med avhør og pågripelse, sier KRIPOS-sjefen"[124]

At politi og påtalemyndigheter søker en så stor verktøykasse som mulig, er naturlig. Samtidig sier sitatet noe om hvor viktig politiet i dag anser trafikkdata for å være. Hvor stor vekt man bør tillegge dette, er vanskelig å si.

Et annet sitat fra media som belyser bruken av trafikkdata i Norge er dette:

> "KRIPOS har dokumentert at det ble innhentet trafikkdata i 52 prosent av 1.450 alvorlige straffesaker - der det ble ilagt straff for drap, narkotikaforbrytelse, ran eller seksuelle overgrep. I 82 prosent av disse sakene hadde trafikkdata stor betydning."[125]

Her fremgår det at KRIPOS har gjort en undersøkelse der trafikkdata har hatt "stor betydning" i 82 prosent av de 754 sakene (52 prosent) der de har blitt forespurt og utlevert. (Jeg har ikke fått tilgang på den originale dokumentasjonen fra KRIPOS, men forutsetter at dette er korrekte data.) Disse dataene er mer presise enn empiriske data nevnt over, og omfatter en snevrere gruppe lovbrudd. Der de tidligere studier har indikert "nytte" i litt under halvparten av sakene, er det her snakk om "stor betydning" i et klart flertall av sakene. Tallene fra de øvrige undersøkelsene baserer seg på alle typer kriminalitet, tallene fra KRIPOS er derimot

123 NOU 2009:15 og Regeringens skrivelse 2009/10:66
124 Aftenposten, 2010, http://www.aftenposten.no/nyheter/iriks/politikk/article3569525.ece
125 Dagsavisen, 2010, http://www.dagsavisen.no/meninger/article489394.ece

fra alvorlige straffesaker alene. Dette er i relasjon til min oppgave mer relevant da grensen for direktivet er "serious crime". Selv om jeg ikke vil legge avgjørende vekt på ubekreftede data, er det klart at denne typen data gir et mer presist inntrykk av situasjonen når det gjelder alvorlig kriminalitet. Det at trafikkdata har stor betydning i mellom 550-600 (av totalt 1450 saker, og av ca 750 saker der data har blitt tillatt uthentet) alvorlige straffesaker årlig, er sådan et viktig moment i relasjon til nytteeffekten av inngrepet.

5.3.5.3 Statistikk fra Danmark og EU forøvrig

Statistikk fra EU og Danmark kan være en god indikator på hvor stor nytte forskjellige myndigheter har av trafikkdata. Når jeg leser statistikk fra Danmark og uttalelser i det upubliserte evalueringsdokumentet fra EU er det noen ting jeg biter meg merke i.[126] I første rekke er det verdt å merke seg at 93 prosent av trafikkdata som uthentes i Danmark er mobildata. Det hentes altså ut forholdsvis lite data fra fasttelefoner, bredbåndstelefoni, Internettepost og ordinær Internettrafikk. Dette har flere implikasjoner. Dette kan være en indikasjon på at direktivets påbud om lagring av fasttelefon-, bredbåndstelefoni-, Internettepost-, og Internettrafikk-data, ikke nødvendigvis utgjør en samfunnsnytte på samme nivå som tilsvarende data for mobiltrafikk og at de tilsvarende ikke samsvarer med et samfunnsbehov. Samtidig indikerer det motsatt at bruken av mobildata som verktøy i straffesaker er en sentral del av politiets basisverktøy når det gjelder bekjempelse av grov kriminalitet i Danmark. Tilsvarende data kan man finne i den upubliserte rapporten fra EU, her fremgår det at 89 prosent av utleverte trafikkdata fra EU er fra mobiltrafikk.[127] Dette kan indikere at lagring av trafikkdata fra de øvrige kommunikasjonsformene ikke nødvendigvis utgjør et utstrakt bidrag til arbeidet politi- og påtalemyndigheter gjør i forbindelse med forebyggende og etterforskende arbeid i Europa forøvrig. Samtidig er det vanskelig å konkludere klart her, statistikken er ikke fordelt på type kriminalitet, og den groveste kriminaliteten kan være fordelt på de 7-10 prosent som gjelder datatrafikk. Likevel gir fordelingen av uthentede data en indikasjon på hvor politiets fokus ligger. I andre rekke fremgår utleveringsstatistikkens tidsramme som en indikator på at lagringstider på 12-24 måneder, slik direktivet åpner for, i mindre grad tilsvarer et samfunnsbehov. De fleste utleveringer skjer både i Danmark og EU forøvrig de første tre måneder. Det er også en større gruppe utlevering mellom tre og seks måneder, men etter seks måneder går utleveringsfrekvensen markant ned. Dette indikerer at samfunnsnytten av å ha lagring på 6-24 måneder ikke nødvendigvis er stor sammenlignet med lagring i opp til 3 måneder. Dette vil jeg gå nærmere inn på i avsnittet om alternative handlemåter.

5.3.5.4 Opprettholdelse av gjeldende situasjon

Et argument man kan anføre til forsvar for å innføre direktivet er at man de siste 15-20 år har hatt tilgang på data lagret av faktureringshensyn. Trafikkdata har sådan vært en tilgjengelig ressurs for bruk i etterforskningsøyemed over lengre tid og vært et verktøy politiet har brukt i

126 JIO Skema logning alle kredse 2009 og Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communication.
127 Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communication. s. 34 (sammensatt statistikk fra et utvalg medlemsland)

flere profilerte norske saker. Her blir av politiet bl.a.Baneheia-saken og Nokas-saken nevnt. (Her kan man dog bemerke at trafikkdataene i Baneheia-saken viste at en av de to hovedtiltalte ikke var i området da drapet skulle ha skjedd og at det i Nokas-saken viste seg at trafikkdata ikke fikk noen stor betydning.) Jo flere leverandører som går fra en tradisjonell faktureringsmodell til fastprisløsninger der man kan ringe/sende så mange meldinger/bruke Internett så mye man ønsker for en fast pris, jo sjeldnere vil data lagret av faktureringshensyn forekomme, dette er i hvert fall et av hovedpremissene for at det foreligger et behov for direktivet. Dette gjør at direktivet opprettholder den gjeldende situasjonen. Det at vi på mange måter i realiteten viderefører en situasjon som har pågått i 10-15 år, tilsier at dette er et mindre inngrep enn om dette var en helt ny praksis som skulle innføres. Politiet får fortsatt tilgang på et verktøy de har brukt aktivt i flere år. Samtidig kan det være verdt å merke seg at direktivet utvider lagringsplikten utover det som tidligere har blitt lagret av faktureringshensyn, data om mottager av datatrafikk er et av flere eksempler her. Det gjør direktivet til noe mer enn en videreføring av en bestående praksis. Selv uten utvidet lagring, er det utvilsomt slik at tvungen lagring av sikkerhetshensyn er noe radikalt annet enn lagring av faktureringshensyn. Dette fremgår bl.a. av Malone-dommen, der det settes en klar grense mellom lagring på tilbydernes hånd med fakturering som motiv og det at disse dataene blir utlevert.[128] Videre kan det være verdt å nevne at en av grunnene til at det nok har vært få lekkasjer og lite misbruk av trafikkdata kan være at dataene har vært lite teknisk tilgjengelig som en følge av måten de blir lagret på. Om direktivinnføringen innebærer at leverandørene kommer til å lagre i to parallelle databaser, en for faktureringshensyn og en direktiv-database der ferdigvaskede og systematiserte data ligger, vil dette gjøre misbruk mer sannsynlig.

5.3.5.5 Dagens praksis i Norge versus en eventuell innføring av direktivet

Dagens ordning i Norge er regulert av Ekomloven.[129] Her fremgår det av § 2-9. Taushetsplikt at oppheving av taushetsplikten i relasjon til trafikkdata, skal godkjennes av Post- og teletilsynet (PTT) "med mindre særlige forhold gjør det utilrådelig". Det er altså ingen terskel for alvorlig kriminalitet eller andre momenter slik man finner det i direktivet. Ser man på høringsdokumentene som har blitt forberedt i forbindelse med høringen om datalagringsdirektivet, vil en innføring medføre langt strengere regler, samt et påbud om utlevering. Slik jeg tolker regelverket gir en opphevelse av taushetspliktene leverandørene en rett til å utlevere data, ikke en plikt. Slik sett vil det være vanskeligere for politi- og påtalemyndigheter å få ut trafikkdata enn slik situasjonen er nå. Det at man ikke bare viderefører praksis, med noen endringer, men også gjør utlevering strengere er ikke et argument per se, men domstolskontroll er i seg selv et poeng i relasjon til proporsjonalitetsvurderingen.

5.3.5.6 Harmonisering av lagringsutgifter for ekomtilbydere

Et av de to hovedformålene med direktivet var å harmonisere tilbydernes konkurransevilkår i forbindelse med lagring av trafikkdata. Det var stor variasjon i lagrings- og sletteplikt blant medlemslandene. Dette ønsket man å fjerne. Har det så blitt like konkurransevilkår?

128 CASE OF MALONE v. THE UNITED KINGDOM (Application no. 8691/79) §§83-85.
129 Lov om elektronisk kommunikasjon (ekomloven). LOV-2003-07-04-83

Direktivet regulerer ikke hvordan lagringsplikten finansieres. Statene velger dermed selv hvordan utgiftene skal fordeles. Dette har ført til at den tidligere situasjon med særs ulike konkurransevilkår, har blitt videreført. Man har ordninger som varierer fra at staten står for alle utgifter (mindretallet) og at statene tar noen utgifter, til at tilbyderne selv står for alle utgifter.[130] I tillegg er det en rekke ordninger som knytter finansiering opp mot kvaliteten på trafikkdata som hentes ut (søkbarhet, format o.l.). Dette gjør at ordningene har ført til en økt konkurransevridning. Dette er en faktor som taler mot at direktivet er et proporsjonalt og nødvendig inngrep.

5.3.5.7 Delkonklusjon

Det synes å være liten tvil om at politi- og påtalemyndigheter har nytte av trafikkdata i sin etterforskningsvirksomhet. Det store spørsmålet er hvor stor nytteeffekten. Det er verdt å gjenta konklusjonene KRIPOS kommer med, der fremgår det at trafikkdata har stor betydning i 82 prosent av de alvorlige straffesaker hvor trafikkdata blir uthentet. Dette kan indikere at trafikkdata er et grunnleggende verktøy med utstrakt bruk og betydning ved alvorlige straffesaker. Dette må det legges vekt på i den videre drøftelse. Dette blir modifisert kraftig om trafikkdatalagring uavhengig av direktivet skulle vise seg å bli realiteten slik IKT-Norge hevder. Videre kan det være verdt å peke på den øvrige statistikken som dokumenterer en lavere grad av nytte, om enn for alle typer kriminalitet. Den første konklusjonen jeg vil komme med her, er at det er et behov for ytterligere forskning på bruk av trafikkdata som etterforskningsverktøy. Slik forskningssituasjonen er nå, er det vanskeligere å sikkert konkludere med at nytten av trafikkdata tilsvarer «a social pressing need», slik praksis fra EMD krever. Tallene fra KRIPOS kan indikere at kriteriene fra rettspraksis er møtt, men jeg vil nødig basere en delkonklusjon på dette alene.

Kort tilslutt vil jeg gå litt nærmere inn på de store variasjoner innad blant medlemslandene i EU og EØS når det gjelder behov for direktivet. De forskjeller som foreligger når det gjelder kriminalitetsnivå kan føre til at direktivet anses som et proporsjonalt og nødvendig inngrep i noen av landene som er øverst på statistikken over grov kriminalitet, samtidig som man i forhold til land som Norge og Danmark ikke nødvendigvis vil komme til samme konklusjon. Jeg må forholde meg til den situasjon som foreligger i Norge.

5.3.6 Alternative handlemåter

5.3.6.1 Innledning

Som nevnt over, er ikke det at det foreligger alternative handlemåter i seg selv et avgjørende moment. Det er kun en av flere faktorer som må tas med i drøftelsen. Jeg vil her se på momenter ved direktivimplementeringen hos forskjellige medlemsland som er verdt å kommentere i denne sammenhengen. Hvis direktivet som helhet eller enkeltdeler av direktivet kan endres for å gjøre inngrepet mindre alvorlig samtidig som man oppnår samme grad av måloppfyllelse, er dette et tungtveiende argument mot en harmonisering av EMK art. 8 og direktivet.

130 Room Document - Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communications

5.3.6.2 Lagringstid

Når det gjelder lagringstid, kan det være naturlig å peke på den ennå ikke offisielt publiserte rapporten om datalagringsdirektivet internt i EU.[131] Brorparten av data blir uthentet de første tre måneder, de følgende tre (3-6 måneder) blir også en merkbar mengde hentet ut, men etter seks måneder faller utleveringsfrekvensen kraftig. Den gjennomsnittlige påbudte lagringstid i EU er tolv måneder. Dataene fra rapporten kan indikere at nytten av trafikkdata markant synker når man overstiger seks måneder, tendensen forsterkes når man overstiger tolv måneder, med svært få uthentinger av data mellom tolv og tjuefire måneder. Disse dataene er i stor grad samsvarende med de data jeg har fått tilgang på fra Danmark.

Det kan etter dette være naturlig å se på nye tidsrammer for lagringen av trafikkdata. Det kan være nærliggende å anta at inngrepet denne lagringen utgjør vil ha færre og mindre omfattende konsekvenser hvis man korter ned lovlig lagringstid fra seks til tjuefire måneder til tre til seks måneder eller to til åtte måneder. Man kan ikke tillegge en nedkorting av lagringstiden avgjørende vekt, men samtidig er det verdt å merke seg at dette kan være et felt hvor man kan minske konsekvensene, uten at inngrepets effekt og målsetning påvirkes i stor grad. De undersøkelser som er gjort i Tyskland rundt nettbruk og bruk av andre kommunikasjonsmidler har ikke vært inne på spørsmål rundt eventuelt minsket lagringstid, men min hypotese er at mange vil oppfatte markant kortere lagringsperioder som mindre inngripende. Ser man hen til Monory-saken kan det være naturlig å se på bruken av personlige data som bevis i denne saken i samme lys som lagring av trafikkdata utover seks måneder.[132] Altså et virkemiddel som i liten grad bidrar til den ønskede effekten. Det er vanskelig å se en avgjørende kriminalitetsbekjempende effekt av lagringen utover seks måneder, målet om kriminalitetsbekjempelse blir i all hovedsak dekket av lagring opp til seks måneder. Det kan dermed være naturlig å anta at EMD vil anse lagringstid utover dette for å være mindre nødvendig. Dette punktet kan vanskeliggjøre en harmonisering. Det taler i hvert fall for en minimumsinnføring (lagring i seks måneder).

5.3.6.3 Kategorier av lagrede data

Hvilke data som lagres er også et relevant moment når det gjelder alternative handlemåter. Kan man innskrenke datakategoriene som blir lagret uten å miste markant effekt av direktivet? Som det fremgår av den ikke-publiserte evalueringsrapporten fra EU, er det hovedsaklig mobildata som ønskes utlevert i forbindelse med direktivet.[133] Tilsvarende var det i Danmark i 2009 3761 utleveringer av mobildata, versus 284 utleveringer i alle andre kategorier.[134] Over 90 prosent av utleveringene var rettet mot mobildata. Dette kan indikere at et alternativ kan være å begrense lagringskategoriene. Det at alle andre kategorier i Danmark utgjør rundt 7 prosent av utleveringene, indikerer at man i mindre grad har nytte av denne typen data. Hvis man ved å begrense lagringsinformasjon til kun å innebære mobildata reduserer merkbare deler av inngrepets konsekvenser, samtidig som det ikke i like stor grad reduserer nytteeffekten, er dette en faktor EMD kan komme til å legge vekt på. Ytterlige forskning på

131 Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communication.

132 CASE OF MONORY v. ROMANIA AND HUNGARY (Application no. 71099/01)

133 Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communication

134 JIO Skema logning alle kredse 2009

dette området kan dermed være viktig. De data som er tilgjengelige sier lite i detalj rundt hvilke lovbrudd som resulterer i uthenting av hvilke typer data, dette er en feilkilde som kan påvirke analysen min. Hvis det viser seg at de groveste forbrytelsene resulterer i uthenting av trafikkdata, kan det forskyve konsekvensanalysen. Dette er en av flere grunner til at det, som sagt, bør forskes mer på dette.

Jeg vil kort gå litt nærmere inn på hvordan det vil oppleves om man begrenser lagring til å gjelde mobiltelefontrafikk. Som jeg har nevnt tidligere i oppgaven, har Internett, Internettbasert kommunikasjon, forumer og lignende fenomener inntatt en viktig rolle i det moderne demokrati. Om det skulle vise seg at direktivet har tilnærmelsesvis like stor effekt, uten å lagre data i disse kategoriene, kan det være naturlig å anse dette som et fruktbart alternativ.

5.3.6.4 Skranker mot misbruk

Det fremgår av kapittelet om lovkvalitet, at et av EMDs vurderingstema når det gjelder lovkvalitet, er tilstedeværelsen av egnede rettslige skranker. Skranker mot misbruk og vilkårlige inngrep er også et moment i forbindelse med proporsjonalitetsvurderingen. Dette fremgår bl.a. av Leander-dommen der tilstrekkelige skranker mot misbruk gjorde at domstolen ikke anså inngrepet for å bryte med prinsippet om proporsjonalitet.[135] I denne dommen var det sentralt at uavhengige politikere og ombudsmenn var i en posisjon der de kunne etterse lagring og bruk av "hemmelig" informasjon om borgeres (jobbsøkere, dommen gjaldt bruk av fritt tilgjengelig, men lagret og systematisert informasjon om borgere som søkte på potensielt sensitive posisjoner) politiske fortid samt detaljer om eventuell aktivisme o.l. Dette indikerer at det er sentralt at man i forbindelse med datalagringsdirektivet har forskjellige sikkerhetsmekanismer på plass som kan sikre at utlevering skjer i henhold til de regler som foreligger og at bruken av data innad i politi- og påtalemyndigheter er i henhold til de formål data blir hentet ut for. Her kan det altså både være behov for rettslige skranker som vurderer grunnlag for utlevering av trafikkdata, men også ombud eller kontrollkomiteer som kan anse at både lagring hos leverandører og bruk og lagring hos politiet skjer etter de regler som vil foreligge for å kunne harmonisere innføringen av direktivet med EMK art. 8

Hvis man ser nærmere på Leander-dommen, nevner de svenske myndighetene en rekke tiltak som skulle hindre misbruk.[136] EMD fremhever i den sammenheng spesielt politisk deltagelse i "the national police board", oversyn fra "the chancellor of Justice" og parlamentets ombudsmann samt justiskomiteen fra Riksdagen.[137] Det kan synes som at politisk kontroll i flere ledd, spesielt med uavhengige organer så som ombudsmannen og justiskansleren er viktige for utfallet i saken. Denne typen ettersyn gir borgerne som omfattes av inngrepet en rettssikkerhet de uten denne typen mekanismer ikke ville hatt, og bidrar til å øke tilliten til at de vedtak om inngrep som gjøres ikke er av vilkårlig art. Datalagringsdirektivet er et langt mer omfattende og på mange måter mer inngripende tiltak enn det svenske myndigheter i Leander-dommen utsatte sine borgere for, desto viktigere er det å ha gode mekanismer for å

135 CASE OF LEANDER v. SWEDEN (Application no. 9248/81) §§64-67
136 CASE OF LEANDER v. SWEDEN (Application no. 9248/81) §§62-65
137 http://www.jk.se/ - Justitiekanslern ar regeringens hogste ombudsman, på samma satt som Justitieombudsmannen ar riksdagens hogste ombudsman. Justitiekanslern ska varna integriteten och yttrandefriheten samt rattssakerheten i den offentliga verksamheten.

unngå vilkårlige inngrep og misbruk av mulighetene til overvåkning. Det kan være naturlig å anta at et krav etter EMK vil være uavhengige ombud eller tilsyn modellert etter f.eks. Datatilsynet slik det er i dag eller justiskansleren i Sverige. En instans av denne typen ville så få mandat til å etterse både lagringssikkerhet og protokoller hos leverandørene og behandling og sletting av data hos politimyndighetene. Jevnlige kontroller lagt til en uavhengig instans og en gjennomsiktig prosess vil gjøre mye for å minske faren for vilkårlighet og misbruk av data. Jeg har også en hypotese om at borgernes tillit til systemet vil øke om man har en instans som uavhengig av myndighetene kan sikre at regelverk følges. Dette i tillegg til domstolenes kontroll med spesifikke utleveringssøknader fra politi- og påtalemyndigheter. Jeg har ikke fått tilgang på informasjon fra de land jeg har undersøkt når det gjelder lokale/nasjonale datatilsyn og deres tilsynsoppgaver i detalj, men direktivteksten påbyr i artikkel 9 en slik uavhengig "Supervisory authority". Dennes oppgaver inkluderer de oppgaver EMD har vektlagt som viktige bl.a. i Leander-dommen sitert over. Det er dermed lite som tilsier at man ikke kan lovfeste skranker mot misbruk som tilfredsstiller både de krav EMK art. 8 stiller og de krav datalagringsdirektivet stiller.

5.3.6.5 Samme resultat uten påbud

Som nevnt tidligere hevder IKT-Norge at tendensen med mindre utbredt lagring av trafikkdata ikke er reell. Det fremgår av deres høringsbrev at de anser denne begrunnelsen for direktivet for å være feilaktig.[138] Hvis denne påstanden er riktig, slik at det ikke bare vil foreligge trafikkdata uavhengig av direktivet, men i tillegg mest sannsynlig vil foreligge stadig flere og mer detaljerte trafikkdata fordi leverandører søker å ha oversikt over hvilke tilbud som lønner seg, mellomfakturering o.l. forhold, er dette problematisk. Ser man på Monory-dommen fremgår det at et inngrep må tilføre noe nytt, en marginal styrking av beskyttelsen mot grov kriminalitet vil ikke, slik jeg tolker dommen, være tilstrekkelig her.[139] Jeg har ikke hatt mulighet til å verifisere påstandene fra IKT-Norge ytterligere, men forutsatt at disse stemmer, så er dette alene en problemstilling som kan skape store problemer når det gjelder en harmonisering av direktivet og EMK art. 8.

6 Konklusjon

6.1 Innledning

Jeg har i dette kapittelet gått gjennom en rekke faktorer som tradisjonelt har blitt vektlagt av EMD. I dette avsluttende punktet skal jeg prøve å veie disse opp mot hverandre, sammenfatte og forsøksvis konkludere rundt proporsjonalitet og nødvendighet. Jeg vil flere steder påpeke at manglende informasjon gjør det vanskelig å konkludere og at videre forskning er viktig for å belyse problemstillingene. Som det fremgår av den delen av oppgaven som omhandler

138 Høring - datalagring - Oslo, 20.01.2010
139 CASE OF MONORY v. ROMANIA AND HUNGARY (Application no. 71099/01)

skjønnsrommet over, vil jeg i relasjon til harmoniseringen utsette direktivet for en streng rettslig prøving.

6.2 Vurdering

Jeg vil i første rekke gå gjennom de tradisjonelle vurderingstema: konsekvenser, nytte/behov, alternative handlemåter, sikkerhetsmekanismer. Sekundært vil jeg komme inn på forholdet til IKT-Norges uttalelser om fortsatt lagring av trafikkdata uavhengig av direktivet og hvilke konsekvenser dette kan ha. Samt forholdet til et evt. forbud fra EMD mot allmenne overvåkningstiltak uten noen form for individuell kontroll.

Det synes å være utvilsomt at trafikkdata er et nyttig etterforskningsverktøy. Ser man på statistikken jeg har vist til, blir de ofte brukt og resulterer i ca halvparten av tilfellene i en nytteeffekt. I brorparten av tilfellene brukes trafikkdata til å plassere mistenkte på et gitt sted til et gitt tidspunkt. I all hovedsak brukes mobildata til dette. Dette kan selvsagt også brukes i motsatt henseende: man kan klargjøre at noen ikke var på et gitt sted til et gitt tidspunkt fordi deres mobiltelefon ble brukt et helt annet sted. Det er dog en svakhet med trafikkdata: man har ingen garanti for at det var den/de mistenkte som brukte mobiltelefonen, datamaskinen eller en annen enhet som produserer trafikkdata. Dette kan redusere nytten av trafikkdata. Likevel fremkommer det av tidligere drøftelser i oppgaven, at bruken av trafikkdata utgjør en nytte for politiet. Problemstillingen blir å presisere hvor stor nytteeffekten er. Som tidligere nevnt fremgår det i Handyside-dommen at en nytteeffekt ikke er tilstrekkelig for å tilfredsstille de kravene EMD har tolket inn i nødvendighetskravet.[140] Noe mer enn dette må til. Tidligere i oppgaven har jeg sitert KRIPOS. Der fremgikk det at trafikkdata har hatt “stor betydning” for etterforskningen i over 80 prosent av sakene som defineres som “grov kriminalitet”. Dette må sies å tilfredsstille de krav EMD stiller til nyttegrad. Ser man derimot på de andre studier jeg har referert til, foreligger det resultater som tilsier "nytte" i 40-50 prosent av sakene. Det fremgår av Handyside-dommen at man ikke kan kreve at inngrep er uunnværlige, og det er naturlig å anta at “stor betydning” ligger i rommet mellom “nyttig” og “uunnværlig”. Derimot kan man vanskelig anse at de øvrige studier i like stor grad tilsier at nytten trafikkdata utgjør oppfyller de krav EMD stiller i sin praksis. Disse tallene gjelder dog all kriminalitet, ikke bare grov kriminalitet. Dette gjør at tallene fra KRIPOS fremstår som mer relevante. Jeg velger derfor å legge hovedsaklig vekt på konklusjonene fra KRIPOS (med forbehold om at tallene er korrekte). Inngrepet isolert sett synes dermed å tilfredsstille kravet om “nytte”.

Nytten man opplever ved et inngrep kan dog ikke vurderes i et vakuum. Den må vurderes opp mot konsekvensene av inngrepet for å se om det er proporsjonalitet mellom ulemper og fordeler. Her er det flere vurderingstema som er verdt å peke på.

Det første jeg vil peke på er den manglende måloppnåelsen når det gjelder harmonisering av utgifter til trafikkdatalagring. Dette var opprinnelig et av de uttalte formål med direktivet, men den ferdige direktivteksten regulerte ikke finansieringsmodeller. Dette førte til at de land som

140 Handyside v. Uk, 1976

har innført direktivet har finansieringsløsninger som spenner fra delvis eller full statlig finansiering til ingen statlig finansiering. Dette fører til at konkurransesituasjonen for leverandører ikke har bedret seg som følge av direktivet, dette er et poeng som taler i disfavør for en harmonisering av direktivet og EMK art. 8.

Videre må man se nytten av direktivet opp mot potensielle og faktiske negative konsekvenser. Som tidligere nevnt er det få undersøkelser som har kartlagt borgernes kommunikasjonsvaner i etterkant av direktivet. Den ene undersøkelsen jeg har sett nærmere på, indikerer dog at borgerne vil endre vanene sine. Uavhengig av endrede kommunikasjonsvaner er en allmenn lagring av alle borgernes trafikkdata et altomfattende og dyptpløyende inngrep. Det at man i realiteten vil påby kartlegging av alle borgeres geografiske plassering og kommunikasjonsvaner flere ganger daglig er i seg selv en alvorlig konsekvens. Jeg har tidligere i oppgaven vist til tall fra MiT som indikerer at med tilstrekkelig gode programmer for å analysere trafikkdata, så kan man hente ut detaljerte analyser av borgernes vaner, vennekrets, arbeidskolleger og lignende informasjon. Videre har jeg beskrevet EMDs syn på inngrep som utsetter pressens kildevern for fare. Her har domstolen lagt til grunn at selv bekjempelse av grov kriminalitet ikke kan rettferdiggjøre inngrep som setter pressens kildevern i fare. Hvis et av direktivets konsekvenser er at pressens kilder kan komme i fare for å bli avslørt enten via lekkasjer eller uthenting av data i andre saker, så er dette et problem som nok vil veie tungt i disfavør av en mulig harmonisering. Når det gjelder ulempenes satt opp mot fordelene, er det vanskeligere å komme med en klar konklusjon. Det er flere problematiske forhold med en eventuell innføring av direktivet på dette tidspunkt, mest sentralt fremstår manglende dokumentasjon og forskning på konsekvenser. Jeg vil derfor unnlate å komme med en direkte konklusjon her. Jeg vil likevel si at en direktivinnføring ikke fremstår som uproblematisk i relasjon til EMK art. 8 slik situasjonen er i dag.

IKT-Norges kommer i sitt høringsbrev med en uttalelse om at leverandører nok vil fortsette å lagre trafikkdata, sågar med økt detaljnivå, uavhengig av datalagringsdirektivet. Hvis dette viser seg å medføre riktighet, vil direktivet miste hovedvekten av sin nytte og dermed fremstå som langt mindre proporsjonalt. Det er vanskelig å se hvordan direktivet i en slik situasjon kan tilfredsstille de krav EMD stiller til nytteverdi i rettspraksis. Også her er det et behov for ytterligere informasjon. Hvis man legger til grunn at leverandørene uavhengig av direktivet vil lagre trafikkdata i fremtiden, så vil det være et sterkt argument mot en eventuell harmonisering av direktivet og EMK art. 8

De argumenter Wessel-Aas fremmer om allmenn lagring kan også, om de blir tillagt vekt, ødelegge for en mulig harmonisering av EMK art. 8 og datalagringsdirektivet. Både Weber-dommen og Liberty-dommen og de uttalelser som kommer i S and Marper-dommen underbygger hans teori. Spesielt denne uttalelsen fra dommen sett i lys av de to øvrige dommene er illustrerende:

> "the Court is struck by the blanket and indiscriminate nature of the power of retention"

Denne uttalelsen sammenholdt med uttalelsene i Weber and Saravia v. Germany[141] og Liberty and others v. UK[142]-dommene indikerer at all overvåkning av allmenn art, uten at man får en

141 Ikke-publisert
142 CASE OF LIBERTY AND OTHERS v. THE UNITED KINGDOM (Application no. 58243/00)

individuell utsiling eller behandling, ikke vil godtas av EMD. Legger man denne tolkningen til grunn vil en harmonisering av direktivet slik det fremstår i dag og EMK art. 8 være vanskelig. Det kan virke søkt å sammenligne lagring av DNA-profiler med lagring av trafikkdata, men som jeg har vist over, kan man hente ut langt mer personlig informasjon fra trafikkdata enn man kan fra lagrede DNA-data.

Alternative handlemåter utenfor de rammer direktivet setter, bør også vurderes. Her har jeg drøftet både hvilke data som skal lagres, hvor lenge og forholdet til rettslige skranker. Tidsmessig kan man innenfor direktivets påbud legge seg på seks måneder, dette er en lagringsperiode som i forhold til statistikken for utlevering må sies å være innenfor rimelighetens grenser når det gjelder alternative handlemåter. Her er det med andre ord få problemer med å harmonisere direktivet og EMK art. 8. Når det gjelder kategorier av lagrede data er situasjonen en annen. Her er det ikke åpent for å redusere kategoriene av lagrede data i henhold til direktivet. Samtidig viser statistikken at en type data (trafikkdata fra mobiltelefoner) fullstendig dominerer bildet. Dette er dermed en faktor som trekker i negativ retning når det gjelder harmonisering. Det er ikke jf. direktivet rom for å begrense kategoriene lagrede data.

Avslutningsvis vil jeg peke på det faktum at statene har bevisbyrden når det gjelder behovet for inngrep. Statene må tilse at behovet for inngrep er "convincingly established."[143] Dette innebærer bl.a.at det er statenes plikt å belyse forhold som f.eks. IKT-Norges påstand om lagringspraksis. Med den informasjonen jeg har tilgjengelig, kan jeg ikke si at det har blitt gjort tilstrekkelig for å etablere behovet for direktivet på en overbevisende måte i Norge. De høringsutkast og de forarbeider som har blitt tilgjengelig så langt kan ikke sies, slik jeg ser det, å imøtekomme de krav EMD stiller.

Det er sådan flere argumenter både for og mot at en harmonisering kan gjennomføres. To av disse er av en slik natur at hvis man anser dem for korrekte (IKT-Norges uttalelser og Wessel-Aas' tolkning av rettspraksis), så umuliggjør de i praksis en harmonisering. Ser man bort fra disse to, blir situasjonen mer kompleks. Det er liten tvil om at trafikkdata utgjør et nyttig verktøy for politiet. Samtidig er det mangel på presis forskning som beskriver hvor nyttig dette verktøyet er. Det samme kan sies om konsekvensene av direktivet når det gjelder borgernes kommunikasjonsmønstre og pressens kildevern i likhet med en rekke andre faktorer. Hvis jeg skal tillate meg å konkludere, ville jeg lene meg mot å anta at direktivet vanskelig kan harmoniseres med de forpliktelsene Norge har etter EMK art. 8. Dette selv om jeg ser bort fra muligheten om fremtidig lagring uavhengig av direktivet og et syn på rettspraksis som tilsier at allmenn lagring ikke aksepteres av EMD.

6.3 Avsluttende observasjoner

143 CASE OF FUNKE v. FRANCE (Application no. 10828/84)

Avslutningsvis vil jeg komme med noen observasjoner rundt noen problemstillinger knyttet til datalagringsdirektivet. Disse er av en uformell art, men egner seg likevel til å belyse deler av diskursen rundt direktivet.

Det første jeg vil se på, er de typer kommunikasjon som ikke vil falle inn under lagringsplikten i direktivet. Her er det flere former for kommunikasjon som er verdt å nevne. Facebook, Twitter, Gmail, Myspace, Hotmail, Skype, MSN, Linkedin, Flickr og en hel rekke andre forskjellige nettsamfunn er alle utenfor den lagringsplikten direktivet påbyr. Disse var i langt mindre grad utbredt da direktivet ble planlagt, så det er naturlig at slike sosiale medier og kommunikasjonsplattformer ikke ble inkludert. Videre er det vanskelig både teknisk og i forhold til jurisdiksjon å inkludere disse, da da serverne ansvarlig for kommunikasjonen ofte er plassert langt utenfor Norges og EUs grenser. Dette gjør at en veldig stor andel av borgernes kommunikasjon ikke kan knyttes opp mot annet enn oppkoblingstidspunkt og en forholdsvis presis geografisk plassering. Man kan sådan ikke se hvem forskjellige borgere som blir etterforsket for grov kriminalitet har sendt eposter til via Gmail, man kan ikke se hvem de har ringt via Skype og man kan ikke se hvem de har som venner på Facebook. Jeg har ikke tall på hvor mye av trafikken som relateres til denne typen nettsamfunn og sosiale /medier, men tall fra USA kan være illustrerende. Tall fra Comscore viser at 7 prosent av amerikaneres tidsbruk på nettet knyttes til Facebook.[144] Som tall fra 2010 viser, så ligger google.com like bak.[145] Dette indikerer at bare to av aktørene som nevnt over har nesten en sjettedel av all tidsbruk på nettet. Hadde man lagt sammen alle sider av denne typen som ikke vil falle inn under lagringsplikten, kan det være nærliggende å anta at en stor del av nettrafikken vil stamme fra denne gruppen. Dette er et viktig poeng fordi det for det første illustrerer problemet med lovgivning på overvåkningsområdet. Det viser hvor radikalt landskapet kan forandre seg slik at de kart man har designet ikke engang minner om terrenget. I tillegg kan denne tendensen drastisk redusere nytten av trafikkdata som etterforskningsverktøy. Hvis store deler av befolkningens kommunikasjon ikke får frem annen informasjon enn "Person A koblet 18:30 seg opp mot Internett fra sin hjemmemaskin", er min hypotese at dette vil redusere nytten av trafikkdata. Spesielt siden mange husholdninger har flere personer og en rekke enheter bak en enkelt IP-adresse.

Det andre poenget jeg vil belyse står tildels i et motsetningsforhold til det første. Der det første poenget belyser hvordan en stor del av trafikken på Internett ikke vil bli lagret, vil jeg her peke på det motsatte problemet, at en hel mengde data som ikke nødvendigvis lå i lovgivernes tanker da direktivet ble forfattet, vil bli lagret. Per i dag har vi allerede en rekke trådløse enheter som er med oss rundt i hverdagen. Tanken bak direktivet var nok i stor grad å lagre lokasjonsdata og øvrig informasjon knyttet til samtaler og tekstmeldinger fra slike. Slik jeg tolker direktivets ordlyd er en slik konklusjon nærliggende. Slik teknologien har utviklet seg, har dette dog forandret seg radikalt. En smarttelefon kommuniserer med omverden flere ganger i timen, og hver gang den gjør det, vil dens geografiske plassering lagres. Tilsvarende har mange simkortløsninger i alarmer, biler, hytter og i så enkle ting som klokker o.l. Denne tendensen gjør at man ikke bare vil få lagret geografisk plassering når man ringer eller sender tekstmeldinger, men også at ens bevegelser kontinuerlig blir plottet og kan hentes ut i ettertid.

144 http://blog.comscore.com/2010/01/strong_year_for_Facebook.html
145 http://techcrunch.com/2010/03/15/hitwise-says-Facebook-most-popular-u-s-site/

Dette blir et svært finmasket nett og utgjør på mange måter en særs påtrengende form for overvåkning. Av de forarbeidene jeg har lest fremgår det ikke at de som har forfattet direktivet i utgangspunktet har vært inneforstått med potensialet for en slik utvikling. Det samme kan sies om det ordskiftet som har foregått i Norge forut for en eventuell innføring av direktivet. Det synes ikke som at norske politikere i tilstrekkelig grad har forståelse for hva som vil lagres og i hvor stor utstrekning.

Mitt syn er at begge disse problemstillingene tyder på et behov for mer forskning og forståelse for et rettsområde som utvikler seg både teknologisk og i omfang. Dette bør nok være en del av et bredere lovforarbeid før man eventuelt innfører direktivet. Dette i tillegg til faktorer jeg allerede har nevnt: mer forskning på nytten av trafikkdata og innvirkningen på borgernes kommunikasjonsmønster.